D-Link DWL-2600/3600/6600/8600AP

802.11n Unified Access Point

ユーザマニュアル

D-Link
Building Networks for People

安全にお使いいただくために

ご自身の安全を確保し、システムを破損から守るために、以下に記述する安全のための指針をよくお読みください。

安全上のご注意　必ずお守りください

本製品を安全にお使いいただくために、以下の項目をよくお読みになり必ずお守りください。

⚠警告	この表示を無視し、まちがった使いかたをすると、火災や感電などにより人身事故になるおそれがあります。
⚠注意	この表示を無視し、まちがった使いかたをすると、傷害または物損損害が発生するおそれがあります。

記号の意味　⃠ してはいけない**「禁止」**内容です。　❗ 必ず実行していただく**「指示」**の内容です。

⚠警告

分解禁止
分解・改造をしない
機器が故障したり、異物が混入すると、やけどや火災の原因となります。

禁止
落としたり、重いものを乗せたり、強いショックを与えたり、圧力をかけたりしない
故障の原因につながります。

禁止
発煙、焦げ臭い匂いの発生などの異常状態のまま使用しない
感電、火災の原因になります。
使用を止めて、ケーブル / コード類を抜いて、煙が出なくなってから販売店に修理をご依頼してください。

ぬれ手禁止
ぬれた手でさわらない
感電のおそれがあります。

水ぬれ禁止
水をかけたり、ぬらしたりしない
内部に水が入ると、火災、感電、または故障のおそれがあります。

禁止
油煙、湯気、湿気、ほこりの多い場所、振動の激しいところでは使わない
火災、感電、または故障のおそれがあります。

禁止
内部に金属物や燃えやすいものを入れない
火災、感電、または故障のおそれがあります。

禁止
表示以外の電圧で使用しない
火災、感電、または故障のおそれがあります。

禁止
たこ足配線禁止
たこ足配線などで定格を超えると火災、感電、または故障の原因となります。

禁止
設置、移動のときは電源プラグを抜く
火災、感電、または故障のおそれがあります。

禁止
雷鳴が聞こえたら、ケーブル / コード類にはさわらない
感電のおそれがあります。

禁止
ケーブル / コード類や端子を破損させない
無理なねじり、引っ張り、加工、重いものの下敷きなどは、ケーブル / コードや端子の破損の原因となり、火災、感電、または故障につながります。

禁止
正しい電源ケーブル、コンセントを使用する
火災、感電、または故障の原因となります。

禁止
乳幼児の手の届く場所では使わない
やけど、ケガ、または感電の原因になります。

禁止
次のような場所では保管、使用をしない
・直射日光のあたる場所
・高温になる場所
・動作環境範囲外

禁止
光源をのぞかない
光ファイバケーブルの断面、コネクタ、および製品のコネクタをのぞきますと強力な光源により目を損傷するおそれがあります。

⚠注意

❗
静電気注意
コネクタやプラグの金属端子に触れたり、帯電したものを近づけますと故障の原因となります。

❗
コードを持って抜かない
コードを無理に曲げたり、引っ張りますと、コードや機器の破損の原因となります。

❗
振動が発生する場所では使用しない
接触不良や動作不良の原因となります。

禁止
付属品の使用は取扱説明書にしたがう
付属品は取扱説明書にしたがい、他の製品には使用しないでください。機器の破損の原因になります。

電波障害自主規制について

DWL-2600/3600/6600/8600AP は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス B 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。本書の記載に従って正しい取り扱いをしてください。

無線に関するご注意

電波に関するご注意

DWL-2600/3600/6600/8600AP は、電波法に基づく小電力データ通信システムの無線製品として、技術基準適合証明を受けています。従って、本製品の使用する上で、無線局の免許は必要ありません。
本製品は、日本国内でのみ使用できます。
以下の注意をよくお読みになりご使用ください。

◎ この機器を以下の場所では使用しないでください。
- 心臓ペースメーカー等の産業・科学・医療用機器の近くで使用すると電磁妨害を及ぼし、生命の危険があります。
- 工場の製造ライン等で使用されている移動体識別用の構内無線局(免許を必要とする無線局)および特定小電力無線局(免許を必要としない無線局)
- 電子レンジの近くで使用すると、電子レンジによって無線通信に電磁妨害が発生します。

◎ 本製品は技術基準適合証明を受けています。本製品の分解、改造、および裏面の製品ラベルをはがさないでください。

5GHz 帯使用の無線機器に関するご注意

◎ 電波法により、W56 以外の 5GHz 帯 (IEEE 802.11a) は屋外での使用が禁止されています。
◎ 従来の中心周波数（J52）を使用した機器とは通信チャンネルが異なるために通信できません。
◎ 802.11a（W53）使用時は気象レーダー等との電波干渉を避けるためにチャンネルを 自動的に変更する場合があります（DFS 機能）

2.4GHz 帯使用の無線機器の電波干渉に関するご注意

DWL-2600/3600/6600/8600AP の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用している移動体識別用の構内無線局(免許を必要とする無線局)および特定小電力無線局(免許を必要としない無線局)並びにアマチュア無線局(免許を必要とする無線局)が運用されています。

◎ この機器を使用する前に、近くで移動体識別用の構内無線局および特定小電力無線局並びにアマチュア無線局が運用されていないことを確認してください。
◎ 万一、この機器から移動体識別用の構内無線局に対して有害な電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか、または電波の発射を停止してください。
◎ その他、この機器から移動体通信用の特定小電力無線局に対して電波干渉の事例が発生した場合など、何かお困りのことが起きたときは、弊社サポート窓口へお問い合わせください。

使用周波数帯域	2.4GHz 帯
変調方式	DS-SS 方式 /OFDM 方式
想定干渉距離	40m 以下
周波数変更可否	全帯域を使用し、かつ移動体識別用の構内無線局および特定小電力無線局並びにアマチュア無線局の帯域を回避可能

無線 LAN 製品ご使用時におけるセキュリティに関するご注意

無線 LAN では、LAN ケーブルを使用する代わりに、電波を利用してパソコン等と無線アクセスポイント間で情報のやり取りを行うため、電波の届く範囲であれば自由に LAN 接続が可能であるという利点があります。
その反面、電波はある範囲内であれば障害物（壁等）を越えてすべての場所に届くため、セキュリティに関する設定を行っていない場合、以下のような問題が発生する可能性があります。

◎ 通信内容を盗み見られる
悪意ある第三者が、電波を故意に傍受し、以下の通信内容を盗み見られる可能性があります。
- ID やパスワード又はクレジットカード番号等の個人情報
- メールの内容

◎ 不正に侵入される
悪意ある第三者が、無断で個人や会社内のネットワークへアクセスし、以下の行為を行う可能性があります。
- 個人情報や機密情報を取り出す（情報漏洩）
- 特定の人物になりすまして通信し、不正な情報を流す（なりすまし）
- 傍受した通信内容を書き換えて発信する（改ざん）
- コンピュータウィルスなどを流しデータやシステムを破壊する（破壊）

本来、無線 LAN カードや無線アクセスポイントは、これらの問題に対応するためのセキュリティの仕組みを持っていますので、無線 LAN 製品のセキュリティに関する設定を行って製品を使用することで、その問題が発生する可能性は少なくなります。

セキュリティの設定を行わないで使用した場合の問題を充分理解した上で、お客様自身の判断と責任においてセキュリティに関する設定を行い、製品を使用することをお奨めします。

ご使用上の注意

けがや感電、火災および装置の破損のリスクを減らすために、以下の注意事項を遵守してください。

- 保守マーク表示を守ってください。また、ドキュメント類に説明されている以外の方法でのご使用はやめてください。三角形の中に稲妻マークがついたカバー類をあけたり外したりすると、感電の危険性を招きます。筐体の内部は、訓練を受けた保守技術員が取り扱うようにしてください。
- 以下のような状況に陥った場合は、電源ケーブルをコンセントから抜いて、部品の交換をするかサービス会社に連絡してください。
  - 電源ケーブル、延長ケーブル、またはプラグが破損した。
  - 製品の中に異物が入った。
  - 製品に水がかかった。
  - 製品が落下した、または損傷を受けた。
  - 操作方法に従って運用しているのに正しく動作しない。
- 本製品をラジエータや熱源の近くに置かないでください。また冷却用通気孔を塞がないようにしてください。
- 食べ物や飲み物が本製品にかからないようにしてください。また、水気のある場所での運用は避けてください。万一製品が濡れてしまった場合は、トラブルシューティングガイドの該当する文をお読みになるか、サービス会社に連絡してください。
- 本システムの開口部に物を差し込まないでください。内部コンポーネントのショートによる火事や感電を引き起こすことがあります。
- 本製品と一緒にその他のデバイスを使用する場合は、弊社の認定を受けたデバイスを使用してください。
- カバーを外す際、あるいは内部コンポーネントに触れる際は、製品の温度が十分に下がってから行ってください。
- 電気定格ラベル標記と合致したタイプの外部電源を使用してください。正しい外部電源タイプが分からない場合は、サービス会社、あるいはお近くの電力会社にお問い合わせください。
- システムの損傷を防ぐために、電源装置の電圧選択スイッチ（装備されている場合のみ）がご利用の地域の設定と合致しているか確認してください。
  - 東日本では 100V/50Hz、西日本では 100V/60Hz
- また、付属するデバイスが、ご使用になる地域の電気定格に合致しているか確認してください。
- 付属の電源ケーブルのみを使用してください。
- 感電を防止するために、本システムと周辺装置の電源ケーブルは、正しく接地された電気コンセントに接続してください。このケーブルには、正しく接地されるように、3 ピンプラグが取り付けられています。アダプタプラグを使用したり、ケーブルから接地ピンを取り外したりしないでください。延長コードを使用する必要がある場合は、正しく接地されたプラグが付いている 3 線式コードを使用してください。
- 延長コードと電源分岐回路の定格を守ってください。延長コードまたは電源分岐回路に差し込まれているすべての製品の合計定格アンペア数が、その延長コードまたは電源分岐回路の定格アンペア限界の 8 割を超えないことを確認してください。
- 一時的に急激に起こる電力の変動からシステムコンポーネントを保護するには、サージサプレッサ、回線調整装置、または無停電電源装置（UPS）を使用してください。
- ケーブルと電源コードは慎重に取り付けてください。踏み付けられたりつまずいたりしない位置に、ケーブルと電源コードを配線し、コンセントに差し込んでください。また、ケーブル上に物を置いたりしないようにしてください。
- 電源ケーブルやプラグを改造しないでください。設置場所の変更をする場合は、資格を持った電気技術者または電力会社にお問い合わせください。国または地方自治体の配線規則に必ず従ってください。
- システムに対応しているホットプラグ可能な電源装置に電源を接続したり、切り離したりする際には、以下の注意を守ってください。
  - 電源装置を取り付ける場合は、電源装置を取り付けてから、電源ケーブルを電源装置に接続してください。
  - 電源装置を取り外す場合は、事前に電源ケーブルを抜いておいてください。
  - システムに複数の電源がある場合、システムから電源を切り離すには、すべての電源ケーブルを電源装置から抜いてください。
- 製品の移動は気をつけて行ってください。キャスタやスタビライザがしっかり装着されているか確認してください。急停止や、凹凸面上の移動は避けてください。

静電気障害を防止するために

静電気は、システム内部の精密なコンポーネントを損傷する恐れがあります。静電気による損傷を防ぐため、マイクロプロセッサなどの電子部品に触れる前に、身体から静電気を逃がしてください。シャーシの塗装されていない金属面に定期的に触れることにより、身体の静電気を逃がすことができます。

さらに、静電気放出（ESD）による損傷を防ぐため、以下の手順を実行することをお勧めします。

1. 静電気に敏感なコンポーネントを箱から取り出す時は、コンポーネントをシステムに取り付ける準備が完了するまで、コンポーネントを静電気防止包装から取り出さないでください。静電気防止包装から取り出す直前に、必ず身体の静電気を逃してください。

2. 静電気に敏感な部品を運ぶ場合、最初に静電気防止容器またはパッケージに入れてください。

3. 静電気に敏感なコンポーネントの取り扱いは、静電気のない場所で行います。可能であれば、静電気防止床パッド、作業台パッド、および帯電防止接地ストラップを使用してください。

バッテリの取り扱いについて

警告 不適切なバッテリの使用により、爆発などの危険性が生じることがあります。バッテリの交換は、必ず同じものか、製造者が推奨する同等の仕様のものをご使用ください。バッテリの廃棄については、製造者の指示に従って行ってください。

電源の異常について

万一停電などの電源異常が発生した場合は、必ず本スイッチの電源プラグを抜いてください。
電源が再度供給できる状態になってから電源プラグを再度接続します。

安全にお使いいただくために

このたびは、弊社製品をお買い上げいただきありがとうございます。
本書は、製品を正しくお使いいただくための取扱説明書です。必要な場合には、いつでもご覧いただけますよう大切に保管してください。
また、必ず本書、設置マニュアル、および同梱されている製品保証書をよくお読みいただき、内容をご理解いただいた上で、記載事項に従ってご使用ください。

- 本書および同梱されている製品保証書の記載内容に逸脱した使用の結果発生した、いかなる障害や損害において、弊社は一切の責任を負いません。あらかじめご了承ください。
- 本書および同梱されている製品保証書は大切に保管してください。
- 弊社製品を日本国外でご使用の際のトラブルはサポート対象外になります。

なお、本製品の最新情報やファームウェアなどを弊社ホームページにてご提供させていただく場合がありますので、ご使用の前にご確認ください。
また、テクニカルサポートご提供のためにはユーザ登録が必要となります。
http://www.dlink-jp.com/

目次

安全にお使いいただくために 2
静電気障害を防止するために 5
バッテリの取り扱いについて 5
電源の異常について 5

はじめに 9

本マニュアルの対象者 10
表記規則について 10

第 1 章　本製品のご利用にあたって 11

製品概要 11
ポートについて 11
前面パネル（DWL-2600AP） 12
底面 / 側面パネル（DWL-2600AP） 12
前面パネル（DWL-3600AP） 13
上面パネル（DWL-3600AP） 13
前面パネル（DWL-6600AP） 14
底面パネル（DWL-6600AP） 15
前面パネル（DWL-8600AP） 16
上面、下面パネル（DWL-8600AP） 17

第 2 章　アクセスポイントの設置 18

パッケージの内容 18
ネットワーク接続前の準備 18
システム要件 19

第 3 章　アクセスポイントの接続 27

本製品のインストール 27
Web マネージャの画面構成 29
Web マネージャの初期画面 30
Web マネージャのメニュー構成 32
コンソールポートを使用した管理 33
イーサネット設定 35
IEEE 802.1X 認証の設定 36
インストールの確認 37
無線アクセスポイントのセキュリティ設定 37

第 4 章　Status（アクセスポイントステータスの参照） 38

Interfaces（インタフェースステータスの参照） 39
Events（イベントの参照） 40
Transmit/Receive（送受信した統計情報の参照） 43
Client Associations（接続する無線クライアント情報の参照） 45
TSPEC Client Associations（TSPEC クライアント情報の参照） 46
Rogue AP Detection（不正アクセスポイントの検出） 47
Managed AP DHCP（管理アクセスポイントの DHCP 情報の表示） 50
TSPEC Status and Statistics（TSPEC ステータスと統計情報の参照） 50
TSPEC AP Statistics（TSPEC AP 統計情報の参照） 51
Radio Statistics（無線統計情報の参照） 52
Email Alert Status（E メールアラートステータスの参照） 53

第 5 章　Manage（アクセスポイントの管理） 54

Ethernet Settings（イーサネット設定） 55
Wireless Settings（無線設定） 57
Radio（無線の詳細設定） 59
Scheduler Configuration（スケジューラの設定） 63
Scheduler Association Settings（スケジューラ関連設定） 65
VAP（仮想アクセスポイントの設定） 66
WDS（WDS の設定） 74
MAC Authentication（MAC 認証によるアクセス制御） 78
Load Balancing（ロードバランシングの設定） 80
Managed Access Point（管理アクセスポイントの設定） 81
Authentication（802.1X 認証の設定） 83
Management ACL（管理アクセスコントロールリストの作成） 84

第 6 章　Services（アクセスポイントサービスの設定）　85

Web Server（Web サーバの設定）....85
SNMP（アクセスポイントの SNMP 設定）....87
SSH（SSH ステータスの設定）....89
Telnet（Telnet ステータスの設定）....89
QoS（QoS の設定）....90
Email Alert（E メール警告）....92
Time Settings（NTP サーバの有効化）....94

第 7 章　SNMPv3（SNMPv3 の設定）　95

SNMPv3 Views（SNMPv3 ビューの設定）....95
SNMPv3 Groups（SNMPv3 グループの設定）....96
SNMPv3 Users（SNMPv3 ユーザの設定）....97
SNMPv3 Targets（SNMPv3 ターゲットの設定）....98

第 8 章　Maintenance（メンテナンス）　99

Configuration Save（コンフィグレーションの保存）....99
Configuration Restore（コンフィグレーションのリストア）....101
Maintenance（リセットと再起動）....103
Upgrade（ファームウェアの更新）....104
Packet Capture（Packet Capture の設定）....106

第 9 章　Client QoS（クライアント QoS の設定）　111

VAP QoS Parameters（VAP QoS パラメータの設定）....112
Managing Client QoS ACL（クライアント QoS ACL の管理）....113
Class Map（Diffserv クラスマップの作成）....120
Polcy Map（Diffserv ポリシーマップの作成）....125
Client QoS Status（クライアント QoS ステータス）....127
Configuring RADIUS-Assigned Client QoS Parameters（RADIUS クライアント QoS パラメータ）....128

第 10 章　Cluster（アクセスポイントのクラスタリング）　129

Access Points（クラスタによるアクセスポイントの管理）....129
Sessions（クラスタセッションの管理）....132
Channel Management（チャンネルの管理）....133
Wireless Neighborhood（無線近接デバイス情報の参照）....136

第 11 章　ツールメニュー　139

付録 A　設定例　140

VAP の設定....140
無線インタフェースの設定....143
WDS の設定....145
アクセスポイントのクラスタリング....147
クライアント QoS の設定....149

付録 B　システムの初期設定　156

B.1 アクセスポイントの初期設定....156

はじめに

DWL-2600/3600/6600/8600AP ユーザマニュアルは、本製品のインストールおよび操作方法を例題と共に記述しています。

第 1 章 本製品のご利用にあたって

- 本製品の概要とその機能について説明します。また、前面、上面、底面の各パネルと LED 表示について説明します。

第 2 章 アクセスポイントの設置

- 製品の使用要件について説明します。

第 3 章 アクセスポイントの接続

- 製品へのアクセス、IP アドレス、イーサネット設定などの本製品の基本的な設定について説明します。

第 4 章 アクセスポイントステータスの参照

- アクセスポイントのインタフェースについて説明します。

第 5 章 アクセスポイントの管理

- アクセスポイントのイーサネット設定、無線設定、WDS 設定、ロードバランシング、802.1X 認証設定など本製品の管理機能について説明します。

第 6 章 アクセスポイントサービスの設定

- スイッチの Web サーバ設定、SNMP、QoS、NTP の設定について説明します。

第 7 章 SNMPv3 の設定

- 本製品の SNMPv3 設定について説明します。

第 8 章 メンテナンス

- 本製品のメンテナンス方法について説明します。

第 9 章 クライアント QoS の設定

- 無線クライアントからアクセスポイントへのトラフィックに作用する QoS 方法について説明します。

第 10 章 アクセスポイントのクラスタリング

- クラスタによるアクセスポイントの管理方法について説明します。

第 11 章 ツールメニュー

- ツールメニューの使用方法について説明します。

付録 A 設定例

- VAP の設定、無線設定、WDS の設定、アクセスポイントのクラスタリング、クライアント QoS などの設定例について説明します。

付録 B システムの初期設定

- 本製品にあらかじめ設定されている初期値を示します。

本マニュアルの対象者

本マニュアルは、本製品の設置および管理についての情報を記載しています。また、ネットワーク管理の概念や用語に十分な知識を持っているネットワーク管理者を対象としています。

表記規則について

本項では、本マニュアル中での表記方法について説明します。

注意 注意では、特長や技術についての詳細情報を記述します。

警告 警告では、設定の組み合わせ、イベントや手順によりネットワークの接続状態やセキュリティなどに悪影響を及ぼす恐れのある事項について説明します。

表 1 に、本マニュアル中での字体、・記号についての表記規則を表します。

表 1　字体・記号の表記規則

字体・記号	解説	例
「」	メニュータイトル、ページ名、ボタン名。	「Submit」ボタンをクリックして設定を確定してください。
青字	参照先。	" ご使用になる前に "（13 ページ）をご参照ください。
`courier` フォント	CLI 出力文字、ファイル名。	`(switch-prompt)#`
`courier` 太字	コマンド、ユーザによるコマンドライン入力。	**`show network`**
`courier` 斜体	コマンド項目（可変または固定）。	*`value`*
< >	可変項目。< > にあたる箇所に値または文字を入力します。	<*`value`*>
[ ]	任意の固定項目。	[*`value`*]
[< >]	任意の可変項目。	[<*`value`*>]
{ }	{ } 内の選択肢から 1 つ選択して入力する項目。	{*`choice1`* | *`choice2`*}
|（垂直線）	相互排他的な項目。	*`choice1`* | *`choice2`*
Menu Name > Menu Option	メニュー構造を示します。	Device > Port > Port Properties は、「Device」メニューの下の「Port」メニューの「Port Properties」メニューオプションを表しています。

第 1 章　本製品のご利用にあたって

- 製品概要
- ポートについて
- 前面パネル（DWL-2600AP）
- 底面 / 側面パネル（DWL-2600AP）
- 前面パネル（DWL-3600AP）
- 上面パネル（DWL-3600AP）
- 前面パネル（DWL-6600AP）
- 底面パネル（DWL-6600AP）
- 前面パネル（DWL-8600AP）
- 上面、下面パネル（DWL-8600AP）

ここでは、本製品の概要とその機能について説明します。また、前面、上下の各パネルと LED 表示について説明します。

製品概要

D-Link 統合アクセスポイントは、ご使用の無線デバイスとイーサネットデバイス間に安定かつ高速なアクセスを提供します。本製品は、あらゆる規模のビジネス環境において高機能かつ拡張性を兼ね備えた標準ベースの無線ネットワーク向けのソリューションで、最新の無線ネットワーク機能を実現し、WLAN（無線 LAN）の展開を可能にします。

本製品は 2 つのモード、スタンドアロンモードまたは管理モードで操作することができます。

スタンドアロンモード

統合アクセスポイントはネットワークで個々のアクセスポイントとして動作します。管理者は Web ユーザインタフェース（UI）、コマンドラインインタフェース（CLI）、または SNMP を使用することで管理します。

管理モード

統合アクセスポイントは D-Link 統合アクセスシステムの一部となり、統合スイッチを使用して管理を行います。アクセスポイントが本モードの場合、管理用 Web インタフェース、Telnet、SSH、および SNMP サービスは使用できなくなります。

本章では、スタンドアロンモードにした場合の統合アクセスポイントの設定、管理およびメンテナンス方法について詳しく説明します。D-Link 統合スイッチを使用して行う、管理モード時のアクセスポイント設定に関する情報については、スイッチの管理者用マニュアルを参照してください。

DWL-6600AP と DWL-8600AP は IEEE802.11a/b/g/n 対応の 2.4GHz/5GHz デュアルバンド（同時利用）アクセスポイントです。
DWL-2600AP と DWL-3600AP は IEEE802.11b/g/n (2.4 GHz) に対応しており、2.4GHz シングルバンド対応アクセスポイントです。

最初に統合アクセスポイントの電源を入れる前に、以下のセクションを参照して必要なハードウェアやソフトウェアコンポーネント、クライアント設定および互換性について確認してください。新規または拡張する無線ネットワークの立ち上げおよびテストを成功させるために必要なものをあらかじめご用意ください。

DWL-2600AP は販売予定製品です。（2013 年 1 月時点）

ポートについて

- エンドステーション、サーバ、ハブなどのネットワークデバイスとの接続および設定・管理用に 1 ポートの LAN（Auto MDI/MDI-X）ポートを搭載しています。
- LAN ポートは 10M/100M/1000Mbps、半二重 / 全二重間のオートネゴシエーション機能、フローコントロール、および PoE 受電機能をサポートしています。

前面パネル（DWL-2600AP）

本製品の前面パネルには、ステータスを表示する Power LED、WLAN 用の 2.4GHz LED および LAN LED が配置されています。

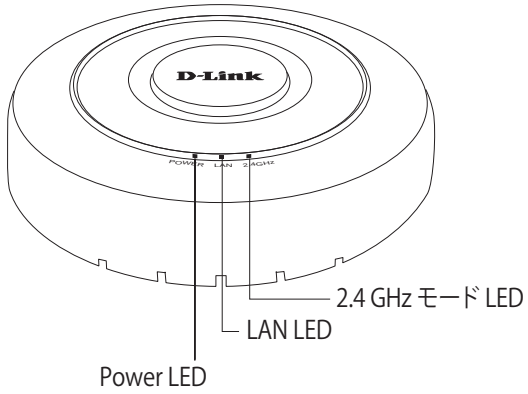


図 1-1　前面パネル図（DWL-2600AP）

ステータス LED は以下の状態を表示します。

LED	色	状態	状態説明
Power	緑	点灯	電源が供給され正常に動作しています。
2.4GHz	緑	点灯	無線 LAN による通信が可能な状態です。
		点滅	無線 LAN によりデータを送受信しています。
LAN	緑	点灯	ネットワークにリンクしています。
		点滅	ネットワーク上でデータを送受信しています。
	ー	消灯	リンクが確立していません。

底面 / 側面パネル（DWL-2600AP）

本製品の底面 / 側面パネルには、リセットボタン、電源ボタン、電源コネクタ、CONSOLE ポートおよび 10BASE-T/100BASE-TX/1000BASE-T（PoE）ポートが配置されています。

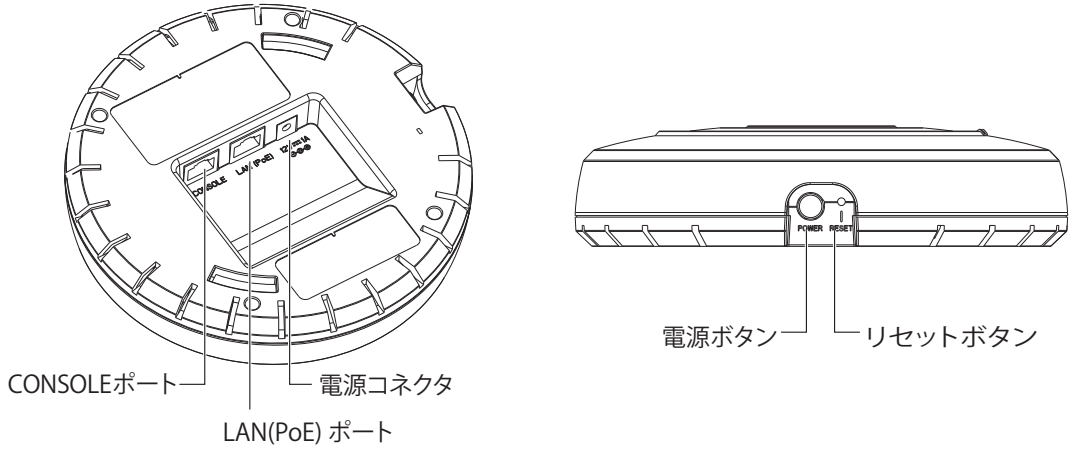


図 1-2　底面 / 側面パネル図（DWL-2600AP）

部位	機能
10BASE-T/100BASE-TX/1000BASE-T（PoE）ポート	RJ-45 コネクタが搭載され、10BASE-T/100BASE-TX/1000BASE-T イーサネットへの接続が可能です。本ポートは NWay プロトコルをサポートしており、ネットワークの伝送速度を検知し、オートネゴシエーションを行います。また、PoE 給電スイッチを使用して受電します。10BASE-T の場合はカテゴリ 3 以上、100BASE-TX の場合はカテゴリ 5 以上、1000BASE-T の場合はエンハンスドカテゴリ 5 以上の UTP/STP ケーブルを接続します。PoE により受電する場合はカテゴリ 5 以上の UTP ストレートケーブルを接続します。
CONSOLE ポート	RJ-45-to-DB9 コンソールケーブルを通じて CLI（コマンドラインインタフェース）にアクセスするのに使用します。
リセットボタン	本製品を工場出荷時設定にリセットします。
電源コネクタ	PoE による受電をしない場合に付属の AC アダプタを接続します。

前面パネル（DWL-3600AP）

本製品の前面パネルには、ステータスを表示する Power LED、WLAN 用の 2.4GHz LED および LAN LED が配置されています。

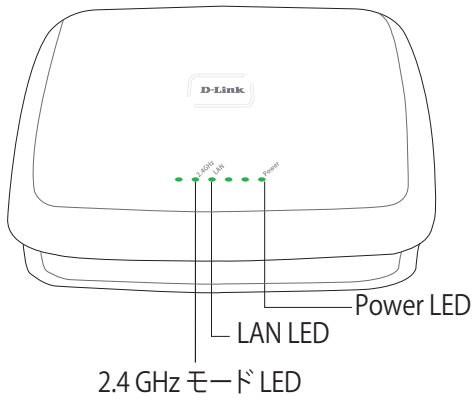


図 1-3　前面パネル図（DWL-3600AP）

ステータス LED は以下の状態を表示します。

LED	色	状態	状態説明
Power	緑	点灯	電源が供給され正常に動作しています。
2.4GHz	緑	点灯	無線 LAN による通信が可能な状態です。
		点滅	無線 LAN によりデータを送受信しています。
LAN	緑	点灯	ネットワークにリンクしています。
		点滅	ネットワーク上でデータを送受信しています。
	ー	消灯	リンクが確立していません。

上面パネル（DWL-3600AP）

本製品の上面パネルには、リセットボタン、電源コネクタ、CONSOLE ポートおよび 10BASE-T/100BASE-TX/1000BASE-T（PoE）ポートが配置されています。

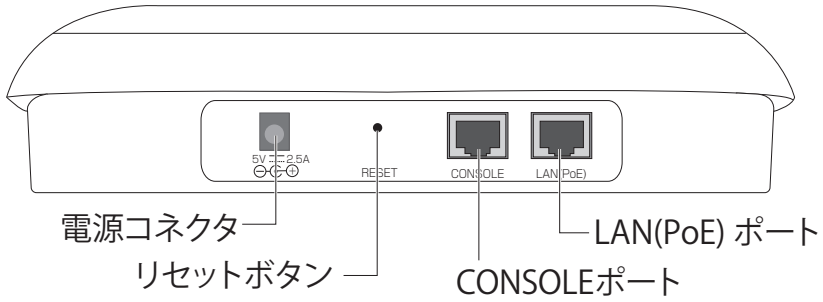


図 1-4　上面パネル図（DWL-3600AP）

部位	機能
10BASE-T/100BASE-TX/1000BASE-T（PoE）ポート	RJ-45 コネクタが搭載され、10BASE-T/100BASE-TX/1000BASE-T イーサネットへの接続が可能です。本ポートは NWay プロトコルをサポートしており、ネットワークの伝送速度を検知し、オートネゴシエーションを行います。また、PoE 給電スイッチを使用して受電します。10BASE-T の場合はカテゴリ 3 以上、100BASE-TX の場合はカテゴリ 5 以上、1000BASE-T の場合はエンハンスドカテゴリ 5 以上の UTP/STP ケーブルを接続します。PoE により受電する場合はカテゴリ 5 以上の UTP ストレートケーブルを接続します。
CONSOLE ポート	RJ-45-to-DB9 コンソールケーブルを通じて CLI（コマンドラインインタフェース）にアクセスするのに使用します。
リセットボタン	本製品を工場出荷時設定にリセットします。
電源コネクタ	PoE による受電をしない場合に付属の AC アダプタを接続します。

前面パネル（DWL-6600AP）

本製品の前面パネルには、ステータスを表示する Power LED、WLAN 用の 5GHz/2.4GHz LED および LAN LED が配置されています。

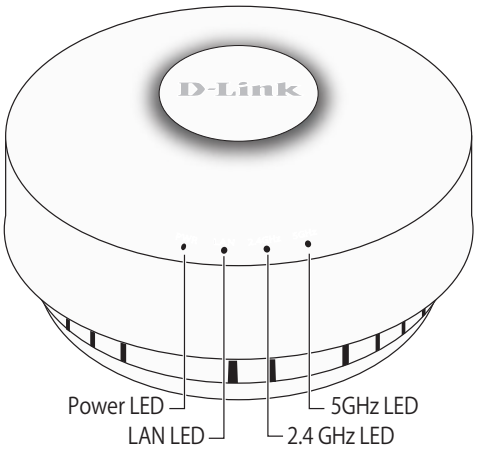


図 1-5　前面パネル図（DWL-6600AP）

ステータス LED は以下の状態を表示します。

LED	色	状態	状態説明
Power	緑	点灯	電源が供給され正常に動作しています。
5GHz	緑	点灯	無線 LAN による通信が可能な状態です。
		点滅	無線 LAN によりデータを送受信しています。
2.4GHz	緑	点灯	無線 LAN による通信が可能な状態です。
		点滅	無線 LAN によりデータを送受信しています。
LAN	緑	点灯	ネットワークにリンクしています。
		点滅	ネットワーク上でデータを送受信しています。
	ー	消灯	リンクが確立していません。

底面パネル（DWL-6600AP）

本製品の上面、底面パネルには、リセットボタン、アンテナ端子、アンテナ選択スイッチ、電源コネクタおよび 10BASE-T/100BASE-TX/1000BASE-T（PoE）ポートが配置されています。

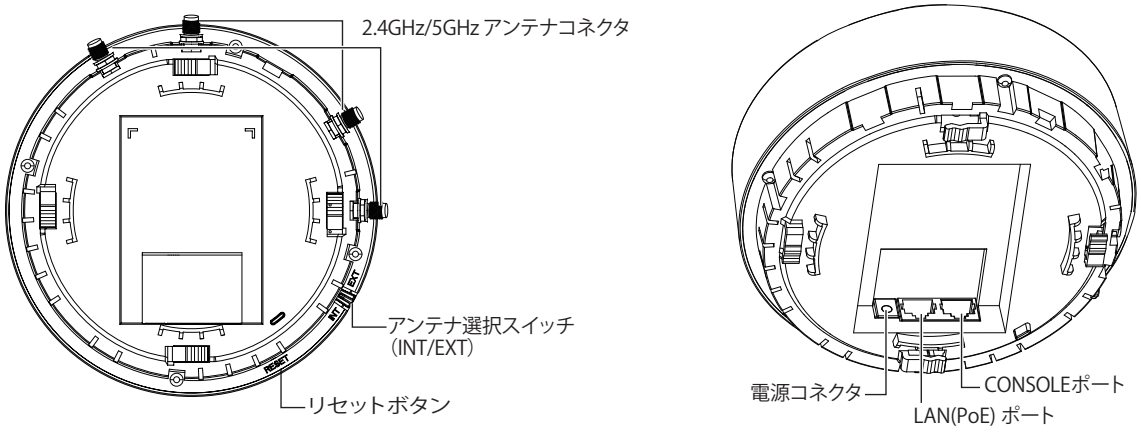


図 1-6　底面パネル図（DWL-6600AP）

部位	機能
10BASE-T/100BASE-TX/1000BASE-T（PoE）ポート	RJ-45 コネクタが搭載され、10BASE-T/100BASE-TX/1000BASE-T イーサネットへの接続が可能です。本ポートは NWay プロトコルをサポートしており、ネットワークの伝送速度を検知し、オートネゴシエーションを行います。また、PoE 給電スイッチを使用して受電します。10BASE-T の場合はカテゴリ 3 以上、100BASE-TX の場合はカテゴリ 5 以上、1000BASE-T の場合はエンハンスドカテゴリ 5 以上の UTP/STP ケーブルを接続します。PoE により受電する場合はカテゴリ 5 以上の UTP ストレートケーブルを接続します。
アンテナ端子	本製品に付属のアンテナを接続します。
アンテナ選択スイッチ	内蔵アンテナを使用する場合は「INT」、外部アンテナを使用する場合は「EXT」を選択します。
CONSOLE ポート	RJ-45-to-DB9 コンソールケーブルを通じて CLI（コマンドラインインタフェース）にアクセスするのに使用します。
リセットボタン	本製品を工場出荷時設定にリセットします。
電源コネクタ	PoE による受電をしない場合に付属の AC アダプタを接続します。

前面パネル（DWL-8600AP）

本製品の前面パネルには、ステータスを表示する Power LED、WLAN 用の 5GHz/2.4GHz LED および LAN LED が配置されています。

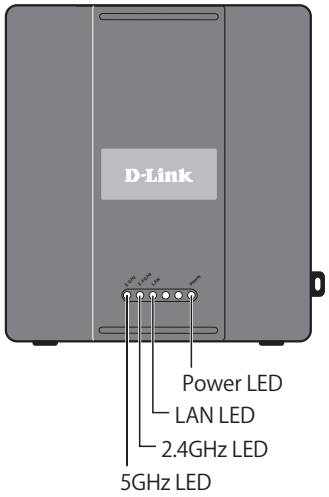


図 1-7　前面パネル図（DWL-8600AP）

ステータス LED は以下の状態を表示します。

LED	色	状態	状態説明
Power	緑	点灯	電源が供給され正常に動作しています。
5GHz	緑	点灯	無線 LAN による通信が可能な状態です。
		点滅	無線 LAN によりデータを送受信しています。
2.4GHz	緑	点灯	無線 LAN による通信が可能な状態です。
		点滅	無線 LAN によりデータを送受信しています。
LAN	緑	点灯	ネットワークにリンクしています。
		点滅	ネットワーク上でデータを送受信しています。
	―	消灯	リンクが確立していません。

上面、下面パネル（DWL-8600AP）

本製品の上面、下面パネルには、リセットボタン、アンテナ端子、電源コネクタおよび 10BASE-T/100BASE-TX/1000BASE-T（PoE）ポートが配置されています。

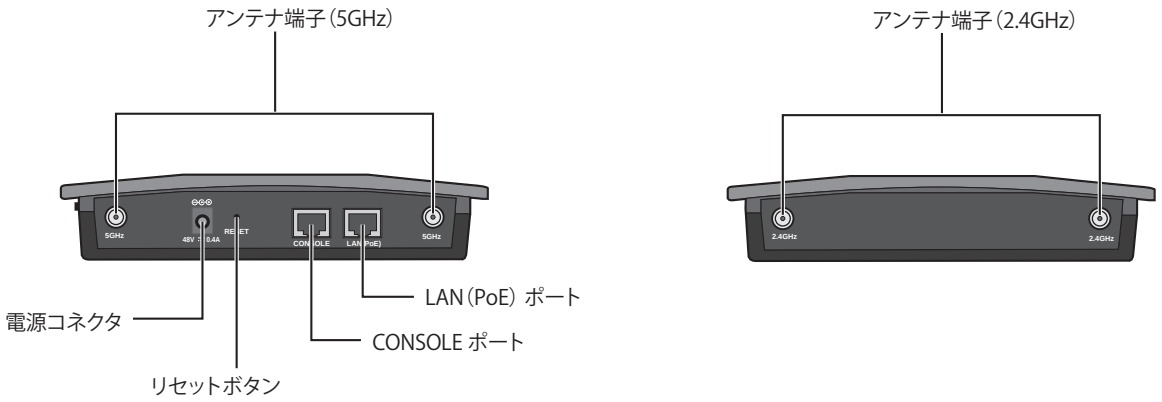


図 1-8　上面、下面パネル図（DWL-8600AP）

部位	機能
10BASE-T/100BASE-TX/1000BASE-T（PoE）ポート	RJ-45 コネクタが搭載され、10BASE-T/100BASE-TX/1000BASE-T イーサネットへの接続が可能です。本ポートは NWay プロトコルをサポートしており、ネットワークの伝送速度を検知し、オートネゴシエーションを行います。また、PoE 給電スイッチを使用して受電します。10BASE-T の場合はカテゴリ 3 以上、100BASE-TX の場合はカテゴリ 5 以上、1000BASE-T の場合はエンハンスドカテゴリ 5 以上の UTP/STP ケーブルを接続します。PoE により受電する場合はカテゴリ 5 以上の UTP ストレートケーブルを接続します。
CONSOLE ポート	RJ-45-to-DB9 コンソールケーブルを通じて CLI（コマンドラインインタフェース）にアクセスするのに使用します。
アンテナ端子	本製品に付属のアンテナを接続します。5GHz 用、2.4GHz に分けて接続します。
リセットボタン	本製品を工場出荷時設定にリセットします。
電源コネクタ	PoE による受電をしない場合に付属の AC アダプタを接続します。

第 2 章　アクセスポイントの設置

- パッケージの内容
- ネットワーク接続前の準備
- システム要件

パッケージの内容

ご購入いただいた製品の梱包箱を開け、同梱物を注意して取り出してください。以下のものが同梱されています。

- 本体　x　1
- アンテナ　x　4（5GHz x 2、2.4GHz x 2）（DWL-8600AP）
- RJ-45/DB9 変換ケーブル　x　1
- ネットワークケーブル　x　1
- PoE 給電アダプタ　x　1（DWL-8600AP のみ）
- AC アダプタ　x　1
- AC 電源ケーブル　x　1（DWL-8600AP のみ）
- マウントキット　x　1
- GNU GPL ライセンスノート　x　1
- シリアルラベル　x　1
- クイックインストールガイド
- CD-ROM　x　1
- 製品保証書

万一、不足しているものや損傷を受けているものがありましたら、弊社ホームページにてユーザ登録を行い、サポート窓口までご連絡ください。

ネットワーク接続前の準備

アクセスポイントの設置場所が性能に大きな影響を与えます。以下のガイドラインに従って本製品を設置してください。

設置にあたってのご注意

本製品の使用により、動作範囲内にて無線でネットワークアクセスが可能になりますが、壁や天井など無線信号が通過する物体の数や厚さ、場所などにより、動作範囲が制約を受ける場合があります。一般的には、構造物の材質や設置場所での無線周波数のノイズが動作範囲に影響を与えます。

1. 本製品と他のネットワークデバイスとの間に入る壁や天井の数をできるだけ少なくしてください。一枚の壁や天井の影響により、本製品の動作範囲は 1 ～ 30 メートルの範囲となります。間に入る障害物の数を減らすようデバイスの位置を工夫してください。

2. ネットワークデバイス間の直線距離にご注意ください。厚さ 50 センチの壁を 45 度の角度で無線信号が通過する時、通り抜ける壁の厚みは約 1 メートルになります。2 度の角度で通過すると、通り抜ける厚みは 14 メートルになります。信号が障害物をなるべく直角に通過するような位置にデバイスを設置し、電波を受信しやすくしてください。

3. 無線信号の通過性能は建築材料により異なります。金属製のドアやアルミの金具などは動作範囲を小さくする可能性があります。無線 LAN デバイスや無線 LAN アダプタ使用のコンピュータの設置は、信号がなるべく乾式壁か開放された戸口などを通るような位置に設置してください。

4. 周波数ノイズを発生する電気機器や家電製品からは、最低でも 1、2 メートル離してデバイスを設置してください。

5. 2.4GHz のコードレス電話または X-10（シーリングファン、ライト、およびホームセキュリティシステムなどの無線製品）を使っている場合、ご使用の無線接続は著しく性能が低下するか、または完全に切断される可能性があります。2.4GHz 電話の親機は可能な限りご使用の無線機器から離れていることを確認してください。電話を使用していない場合でも、親機は信号を送信します。

6. 必ず付属の UTP ケーブル、AC アダプタをご使用ください。

本アクセスポイントは、IEEE 802.3af 準拠の無線スイッチまたは弊社が承認する給電機器から受電することができます。

注意　弊社が承認していない PoE 給電機器に本アクセスポイントを接続すると、本アクセスポイントが破損する場合があります。

システム要件

Web インタフェースを使用、または Telnet や SSH 経由で CLI を使用して統合アクセスポイントを管理するためには、アクセスポイントに IP アドレスが必要になります。また、ネットワーク上で VLAN や IEEE 802.1X 認証を使用している場合、ネットワークに接続する前に、アクセスポイントに追加の設定をする必要があります。

注意 本製品は、インターネットのゲートウェイとして動作しません。ご使用の無線 LAN を他の LAN またはインターネットに接続するためには、別途ゲートウェイが必要です。

管理者用コンピュータ推奨環境

Web ベースのユーザインタフェースを使用して統合アクセスポイントの設定および管理を行うための管理者用コンピュータの最小必要環境を説明します。

1. 本製品へのシリアルまたはイーサネット接続
本製品を最初に設定するためには、使用するコンピュータをシリアルケーブルまたはイーサネットケーブルで接続します。

2. ネットワークへの無線接続
新規の無線ネットワークで最初にアクセスポイントの初期設定および起動を行うと、内部ネットワークへの無線接続を使用して、管理者用 Web 画面で設定変更を行うことができます。
本製品への無線接続には、管理者用機器に無線クライアントと同様の Wi-Fi 機能が必要になります。
- 本製品が準拠する 1 つ以上の IEEE 802.11 モードをサポートする、ポータブルまたは内蔵型の Wi-Fi クライアントアダプタ。
- 本製品と接続するよう設定した無線クライアントソフトウェア。

3. Web ブラウザとオペレーティングシステム
本製品の設定および管理は、本製品に実装された Web ベースユーザインタフェースを経由して行います。
本製品の管理者用 Web 画面に接続するためには、以下のいずれかのブラウザを使用することをお勧めします。
- Microsoft Windows® XP または Microsoft Windows 2000、Microsoft® Internet Explorer® version 5.5 または 6.x 以降
- Redhat® Linux® version 2.4 以降、Netscape Mozilla 1.7.x

管理者用 Web ブラウザは、管理者インタフェースのインタラクティブ機能をサポートするため、必ず JavaScript を有効にしてください。

4. セキュリティ設定
本製品の初期設定に使用する無線クライアントのセキュリティが無効になっていることを確認してください。

無線クライアントの必要環境

統合アクセスポイントは、アクセスポイントが動作している 802.11 モードに対し、Wi-Fi クライアントアダプタが適切に設定されていれば、どんなクライアントにも無線接続を提供します。本製品は、システムを運用している複数のクライアントをサポートします。クライアントとは、Wi-Fi アダプタやサポートドライバが装備されているノートパソコンやデスクトップコンピュータ、PDA、その他の携帯型や据え置き型のデバイスを意味します。

アクセスポイントに接続するためには、無線クライアントに以下に示すソフトウェアおよびハードウェアが搭載されている必要があります。

1. Wi-Fi クライアントアダプタ
アクセスポイントが準拠する 1 つ以上の IEEE 802.11 モードをサポートする、ポータブルまたは内蔵型の Wi-Fi クライアントアダプタ。（IEEE 802.11a、802.11b、802.11g、802.11n をサポート。）

2. 無線クライアントソフトウェア
本製品に接続するよう設定したクライアントソフトウェア（例：Microsoft Windows サプリカント）。

3. クライアントセキュリティ設定
本製品の初期設定を行うために、クライアントのセキュリティは必ず無効にしてください。

本製品のセキュリティモードがテキスト以外で設定される場合、無線クライアントは本製品が使用する認証モードにプロファイルを設定して、有効なユーザ名、パスワード、証明書または同等のユーザ認証を提供する必要が生じます。セキュリティモードとして、スタティック WEP、IEEE 802.1X、RADIUS サーバを持つ WPA および WPA-PSK があります。

本製品のセキュリティ設定に関する情報は、「VAP（仮想アクセスポイントの設定）」（66 ページ）を参照してください。

アクセスポイントのダイナミックおよびスタティック IP アドレス設定

本製品の電源を入れると、実装されている DHCP クライアントは、IP アドレスおよびその他のネットワーク情報を取得するためにネットワーク上の DHCP サーバを検索します。本製品がネットワーク上の DHCP サーバを検出しない場合は、新しいスタティック IP アドレス（スタティック IP アドレッシングポリシー）を割り当てるか、または DHCP サーバからネットワーク情報の受信に成功するまで、引き続きスタティック IP アドレスの初期値（10.90.90.91）を使用します。

接続タイプの変更およびスタティック IP アドレスの割り当てのために CLI を使用する場合は「イーサネット設定」（35 ページ）、Web ユーザインタフェースを使用する場合は「Ethernet Settings（イーサネット設定）」（55 ページ）を参照してください。

注意 ご使用の内部ネットワークに DHCP サーバが存在しない場合、または DHCP サーバを使用しない場合は、電源を投入後、まず接続タイプを DHCP からスタティック IP に変更してください。アドレスの初期値を使用して、本製品に新しいスタティック IP アドレスを割り当てることもできます。同じネットワークに別の WLAN アクセスポイントを導入する場合には各アクセスポイントの IP アドレスが異なるものになるように、新しいスタティック IP アドレスを割り当てることをお勧めします。

IP アドレスのリカバリ

本製品の接続に問題がある場合は、アクセスポイントの設定を工場出荷時の初期値にリセットしてスタティック IP アドレスを回復することができます（「Maintenance（リセットと再起動）」（79 ページ）を参照してください）。または、DHCP サーバを持つネットワークにアクセスポイントを接続して、ダイナミックにアドレスを割り当てることもできます。

ダイナミックに割り当てられた IP アドレスの検出

ご使用のネットワーク上の DHCP サーバに接続してアクセスポイントの IP アドレスを取得すると、アクセスポイントの MAC アドレスに接続する新しい IP アドレスを参照することができます。

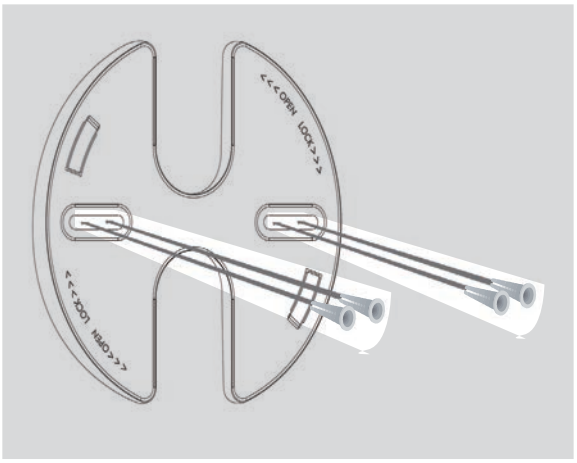
アクセスポイントに IP アドレスを割り当てる DHCP サーバに接続できない場合、またはアクセスポイントの MAC アドレスが不明の場合は、CLI を使用して新しい IP アドレスを検出する必要があります。ダイナミックに割り当てられた IP アドレスの検出については、「CLI を使用した IP アドレスの参照」（33 ページ）を参照してください。

ウォールマウントキットによる壁面への設置（DWL-2600AP）

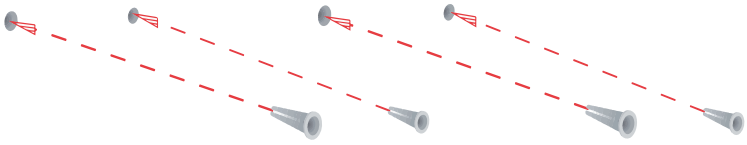
準備：ウォールマウントキットを使用して本製品を壁面に設置するために以下のものをご用意ください。

- ウォールマウントキット（ウォールマウントキット）
- 付属の本体をウォールマウントキットに取り付けるネジ
- 付属のウォールマントキットを壁面に取り付けるネジとアンカー

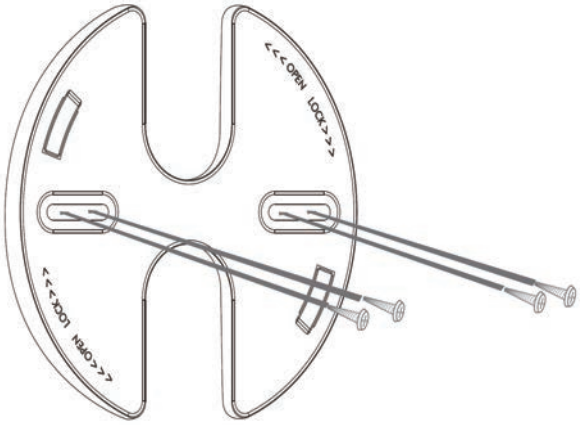
1. ウォールマウントキットを取り付ける壁面に合わせて、本体の向きを調整します。同時にアンカーとネジを差し込む 4 つの位置を確認し、穴を開けます。



2. 壁面にアンカーを挿入する
ウォールマウントキットを設置する壁面に付属のアンカーを挿入します。



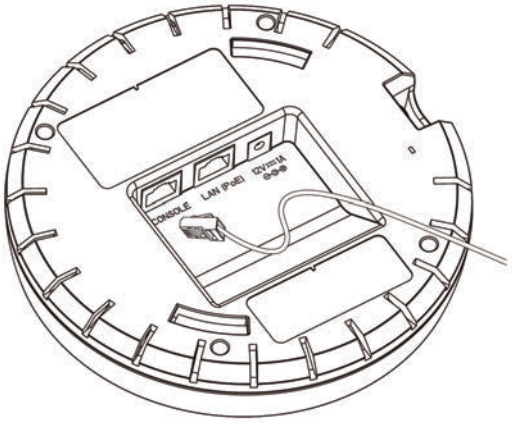
3. 穴を開けた壁面にウォールマウントキットを取り付ける
ウォールマウントキット取り付け用のネジを使用し、4 箇所のウォールマウントキットのネジ穴とアンカーの穴を合わせて、ネジで取り付けます。



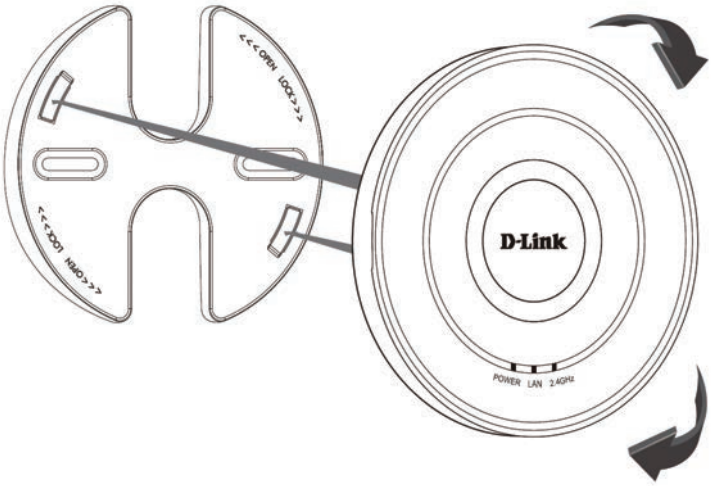
注意 ウォールマウントキットの取り付け位置はアンテナの長さを考慮し、障害物や天井にぶつからない場所にしてください。

注意 石膏ボードやベニヤなどに設置する場合は、あらかじめ壁の厚さを確認の上、きりやドリルで穴をあけて付属のアンカーボルトを埋め込んだ後にネジを取り付けてください。

4. 本体の LAN ポートにケーブルを取り付ける



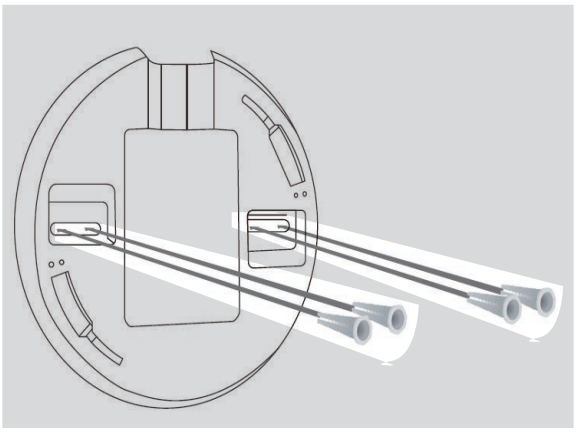
5. 本製品を壁面に取り付ける
本体のフック部分とウォールマウントキットのフック部分を合わせて、本体を右に回して引っかけます。ウォールマウントキット設置時に決めた LED 位置の向きを参考にします。



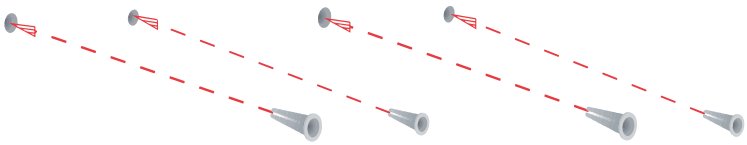
ウォールマウントキットによる壁面への設置（DWL-3600AP）

準備：ウォールマウントキットを使用して本製品を壁面に設置するために以下のものをご用意ください。
- ウォールマウントキット（ウォールマウントキット）
- 付属の本体をウォールマウントキットに取り付けるネジ
- 付属のウォールマントキットを壁面に取り付けるネジとアンカー

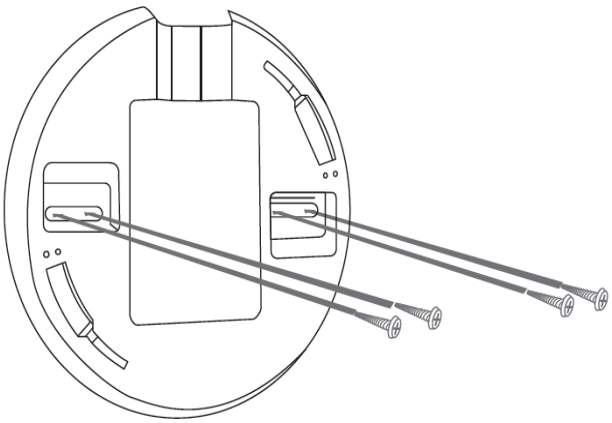
1. ウォールマウントキットを取り付ける壁面に合わせて、本体の向きを調整します。同時にアンカーとネジを差し込む 4 つの位置を確認し、穴を開けます。



2. 壁面にアンカーを挿入する
ウォールマウントキットを設置する壁面に付属のアンカーを挿入します。



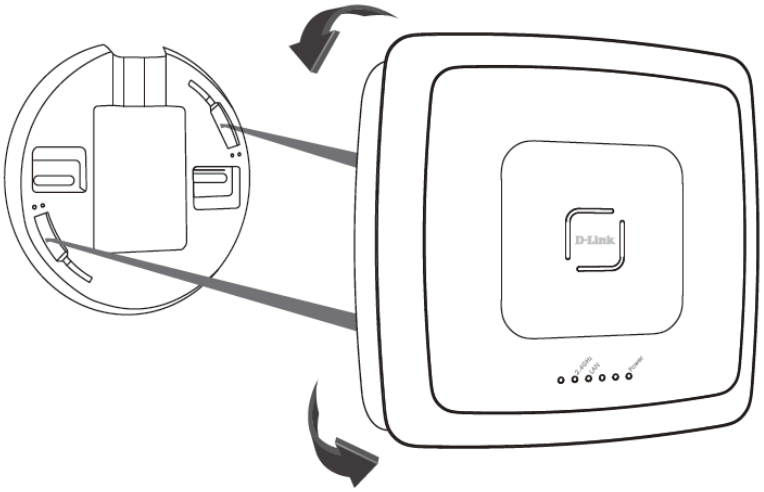
3. 穴を開けた壁面にウォールマウントキットを取り付ける
ウォールマウントキット取り付け用のネジを使用し、4 箇所のウォールマウントキットのネジ穴とアンカーの穴を合わせて、ネジで取り付けます。



注意 ウォールマウントキットの取り付け位置はアンテナの長さを考慮し、障害物や天井にぶつからない場所にしてください。

注意 石膏ボードやベニヤなどに設置する場合は、あらかじめ壁の厚さを確認の上、きりやドリルで穴をあけて付属のアンカーボルトを埋め込んだ後にネジを取り付けてください。

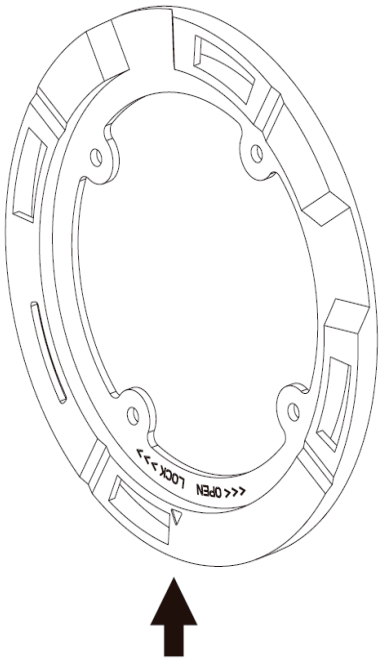
4. 本製品を壁面に取り付ける
本体のフック部分とウォールマウントキットのフック部分を合わせて、本体を左に回して引っかけます。ウォールマウントキット設置時に決めた LED 位置の向きを参考にします。



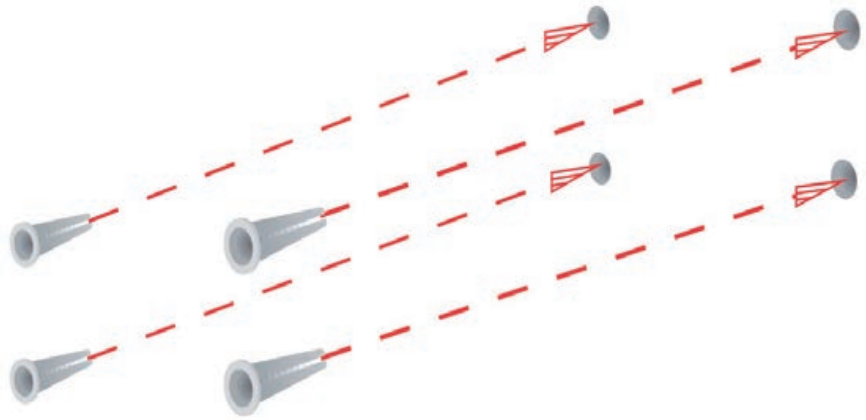
ウォールマウントキットによる壁面への設置（DWL-6600AP）

準備：ウォールマウントキットを使用して本製品を壁面に設置するために以下のものをご用意ください。
- ウォールマウントキット（ウォールマウントキット）
- 付属の本体をウォールマウントキットに取り付けるネジ
- 付属のウォールマントキットを壁面に取り付けるネジとアンカー

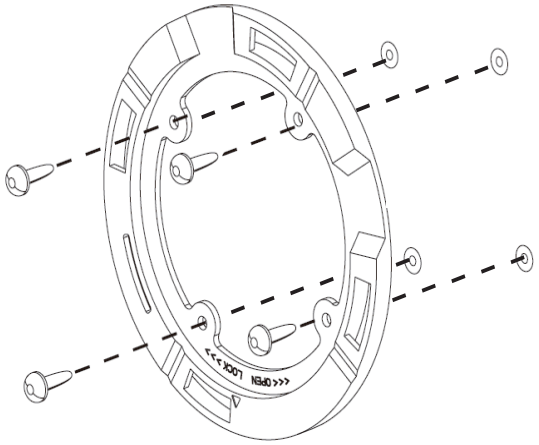
1. ウォールマウントキットを取り付ける壁面に合わせて、前面パネル（LED 部）の向きを調整します。図内の矢印の位置に本体の前面パネル（LED 部）が来ます。同時にアンカーとネジを差し込む 4 つの位置を確認し、穴を開けます。



2. 壁面にアンカーを挿入する
ウォールマウントキットを設置する壁面に付属のアンカーを挿入します。



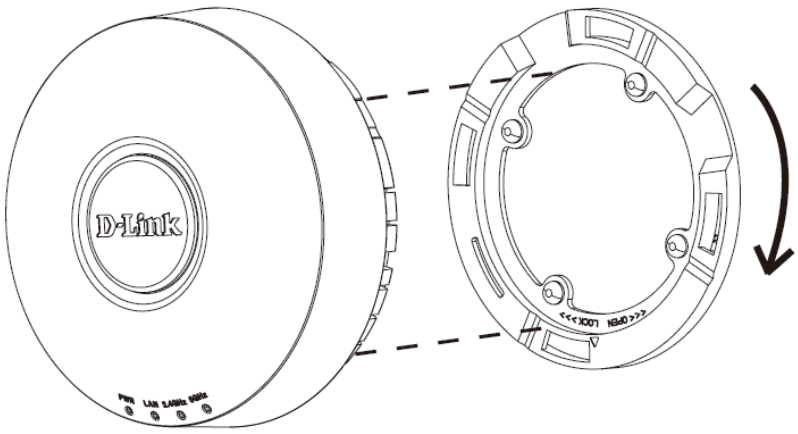
3. 穴を開けた壁面にウォールマウントキットを取り付ける
ウォールマウントキット取り付け用のネジを使用し、4 箇所のウォールマウントキットのネジ穴とアンカーの穴を合わせて、ネジで取り付けます。



注意 ウォールマウントキットの取り付け位置はアンテナの長さを考慮し、障害物や天井にぶつからない場所にしてください。

注意 石膏ボードやベニヤなどに設置する場合は、あらかじめ壁の厚さを確認の上、きりやドリルで穴をあけて付属のアンカーボルトを埋め込んだ後にネジを取り付けてください。

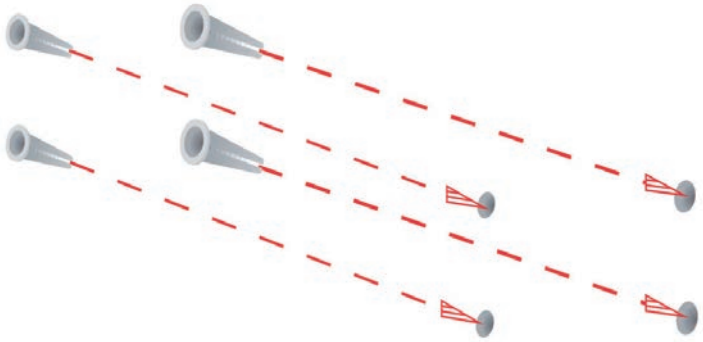
4. 本製品を壁面に取り付ける
本体のフック部分とウォールマウントキットのフック部分を合わせて、本体を右に回して引っかけます。ウォールマウントキット設置時に決めた LED 位置の向きを参考にします。



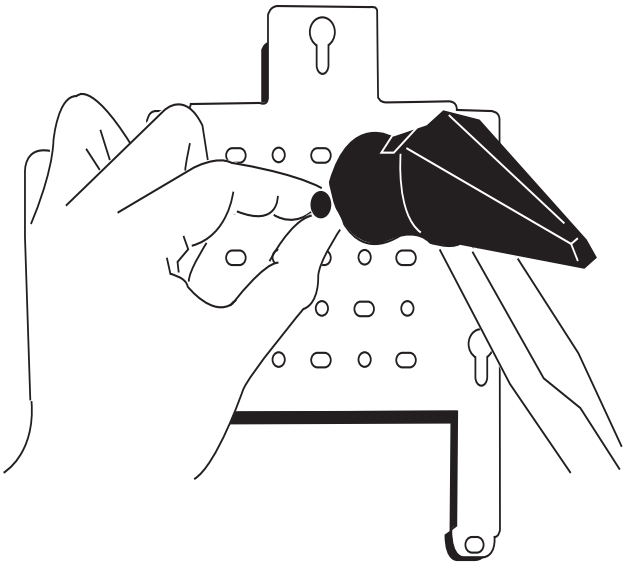
ウォールマウントキットによる壁面への設置（DWL-8600AP）

準備：ウォールマウントキットを使用して本製品を壁面に設置するために以下のものをご用意ください。
- ウォールマウントキット
- 付属の本体をウォールマウントキットに取り付けるネジ
- 付属のウォールマントキットを壁面に取り付けるネジとアンカー

1. 壁面にアンカーを挿入する
ウォールマウントキットを設置する壁面に付属のアンカーを挿入します。



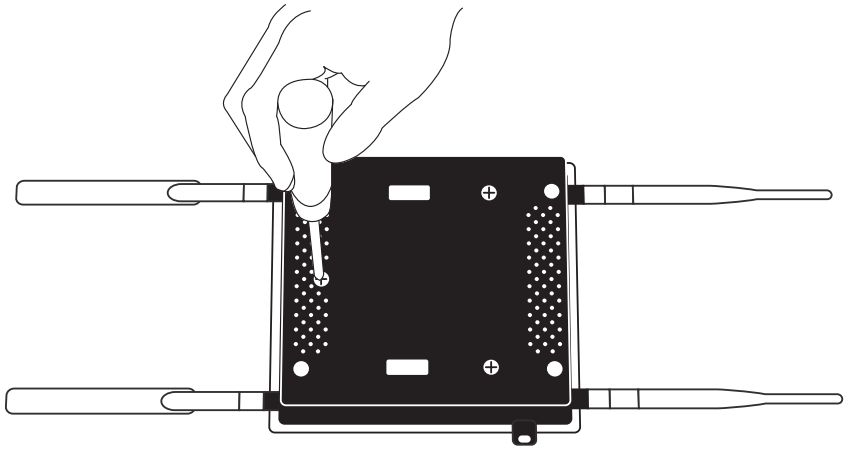
2. 壁面の適切な場所にウォールマウントキットを取り付ける
ウォールマウントキット取り付け用のネジとアンカーを使用し、ウォールマウントキット中央のいずれかのネジ穴にあわせてを取り付けます。



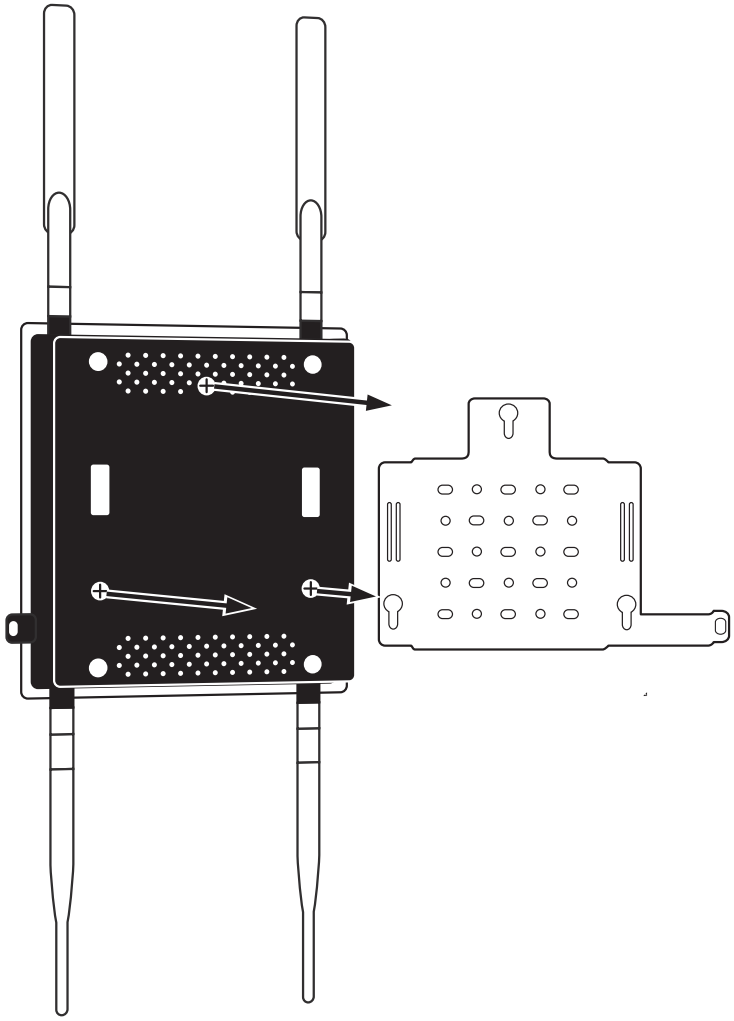
注意 ウォールマントキットの取り付け位置はアンテナの長さを考慮し、障害物や天井にぶつからない場所にしてください。

注意 石膏ボードやベニヤなどに設置する場合は、あらかじめ壁の厚さを確認の上、きりやドリルで穴をあけて付属のアンカーボルトを埋め込んだ後にネジを取り付けてください。

3. 本製品背面に付属のフック用ネジを取り付ける
残りのネジを使用してラックマウントキットに設置するため、ネジと本体にわずかな隙間があるように取り付けます。



4. 本製品を壁面に取り付ける
本製品に取り付けたフック用ネジの頭を、壁に設置したラックマウントキットの 3 カ所の鍵穴に引っかけます。



第 3 章　アクセスポイントの接続

- 本製品のインストール
- Web マネージャの画面構成
- Web マネージャの初期画面
- Web マネージャのメニュー構成
- コンソールポートを使用した管理
- イーサネット設定
- IEEE 802.1X 認証の設定
- インストールの確認

本製品のインストール

管理者用 Web ユーザインタフェースにアクセスするためには、本製品の IP アドレスを Web ブラウザに入力します。IP アドレスの初期値を使用し、アクセスポイントにログインしてスタティック IP アドレスを割り当てるか、ご使用のネットワークにある DHCP サーバを使用してネットワーク情報をアクセスポイントに割り当てることが可能です。初期設定では、アクセスポイントの DHCP クライアントは有効です。

以下の手順で本製品をインストールします。

1. LAN 経由または直接接続することにより、本製品を管理者用コンピュータに接続します。

LAN 接続の場合

以下の図のように、イーサネットケーブルの一端を本製品の LAN ポートに接続し、もう一端をご使用のコンピュータが接続しているハブに接続します。

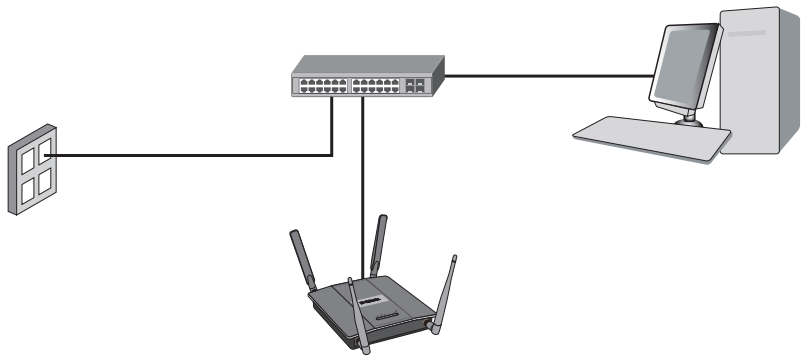


図 3-1　LAN 接続の場合

使用するハブまたはスイッチは、必ずアクセスポイントからのブロードキャスト信号がネットワーク上の他のすべてのデバイスに送信されるのを許可するようにしてください。

UTP ケーブルで直接接続する場合

以下の図のように、UTP ケーブルでアクセスポイントの LAN ポートと PC の LAN ポートに接続します。または、同梱のシリアルケーブルを使用してアクセスポイントのシリアルポートと管理コンピュータを接続します。

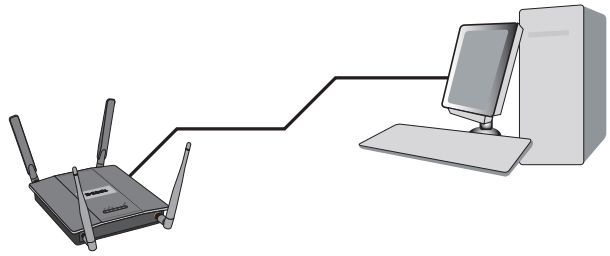


図 3-2　直接接続する場合

DHCP サーバを使用せずに直接イーサネット接続で初期設定を行う場合は、アクセスポイントの IP アドレスの初期値と同じサブネット内のスタティック IP アドレスを持つことを確認してください。（本スイッチの IP アドレスの初期値は 10.90.90.91 です。）

この方法で設定を行った後、アクセスポイントの起動および実際の運用をするためには、上記のどちらの場合も設定用 PC との接続を切り離してネットワークと接続します。

注意　無線接続でネットワーク上のアクセスポイントを検出することも可能ですが、無線による方法をお勧めしません。多くの場合、意図したアクセスポイントに実際接続しているかが不明確なためです。また、無線接続では、必要とされる初期設定の変更がアクセスポイント接続を切断する原因となる場合があります。

2. 本製品底面の電源コネクタに AC アダプタを接続し、電源プラグをコンセントに接続します。

3. Web ブラウザを使用して本製品の管理者用 Web 画面にログインします。

- ネットワーク上の DHCP サーバから IP アドレスを取得しない場合は、ブラウザのアドレスに IP アドレスの初期値「10.90.90.91」を入力します。

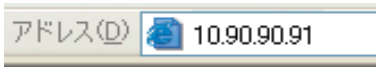


図 3-3　URL の入力画面

- ご使用のネットワークで DHCP サーバを使用していて自動的にネットワーク情報が設定される場合は、Web ブラウザに本製品の新しい IP アドレスを入力します。

- DHCP サーバを使用し、新しい IP アドレスがわからない場合は、以下の手順に従い情報を取得してください。

  - 管理者コンピュータとアクセスポイントをシリアルケーブルで接続し、端末エミュレーションソフトウェアを使用して CLI（command-line interface）に接続します。
  - ログイン画面で、ユーザ名およびパスワードに「admin」と入力します。プロンプトが表示されたら、「get management」と入力します。コマンド出力としてアクセスポイントの IP アドレスが表示されます。このアドレスを Web ブラウザのアドレスに入力してください。

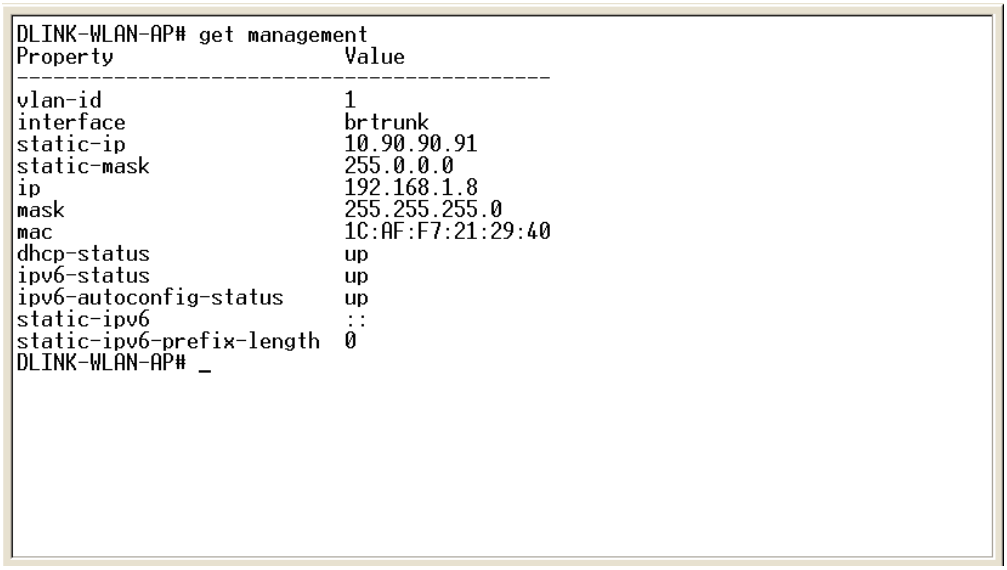


図 3-4　get management 画面

コンソールポートを使用して CLI にログインする方法に関する詳細は、「CLI を使用した IP アドレスの参照」（33 ページ）を参照してください。

4. 以下のユーザ認証画面が表示されます。

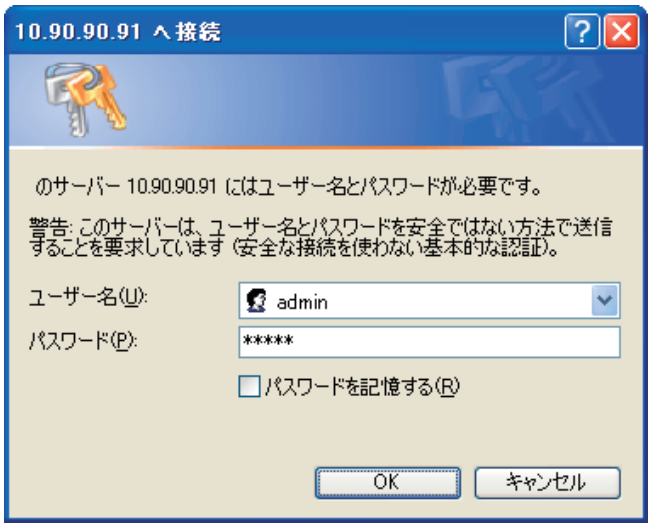


図 3-5　ログイン用画面

「ユーザー名」と「パスワード」に「admin」を入力し、「OK」をクリックして Web ベースユーザインタフェースに接続します。
CLI でパスワードを既に設定している場合は、設定した項目を入力します。

Web マネージャの画面構成

Web マネージャで本製品の設定または管理画面にアクセスすることができます。

Web マネージャのメイン画面について

Web マネージャのメイン画面は 3 つのエリアで構成されています。

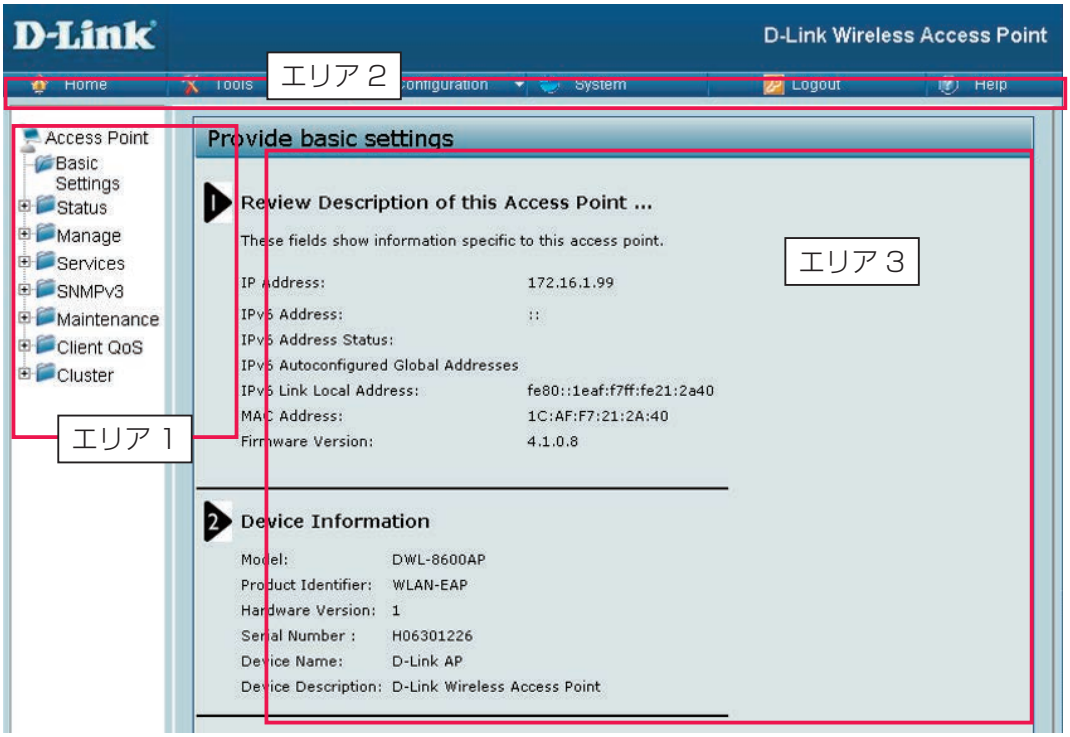


図 3-6　Web マネージャのメイン画面

エリア	機能
エリア 1	表示するメニューまたは画面を選択します。メニューアイコンを開いて、ハイパーリンクしたメニューボタンの表示や、それらを格納するサブメニューを表示します。D-Link のロゴをクリックすると D-Link のホームページに接続します。
エリア 2	本製品の再起動、コンフィグレーションの保存と復元、ファームウエアの更新などを行うメニューがあります。
エリア 3	選択した製品情報の表示と設定データの入力を行います。

Web マネージャの初期画面

Web マネージャが表示されると、メイン画面には本デバイスの基本情報 が表示されます。本画面で現在のデバイスの状態を確認することができます。

Basic Settings（デバイス情報）

IP および MAC アドレス情報など、本製品のさまざまな情報の参照、および管理者パスワードの設定を行うことができます。

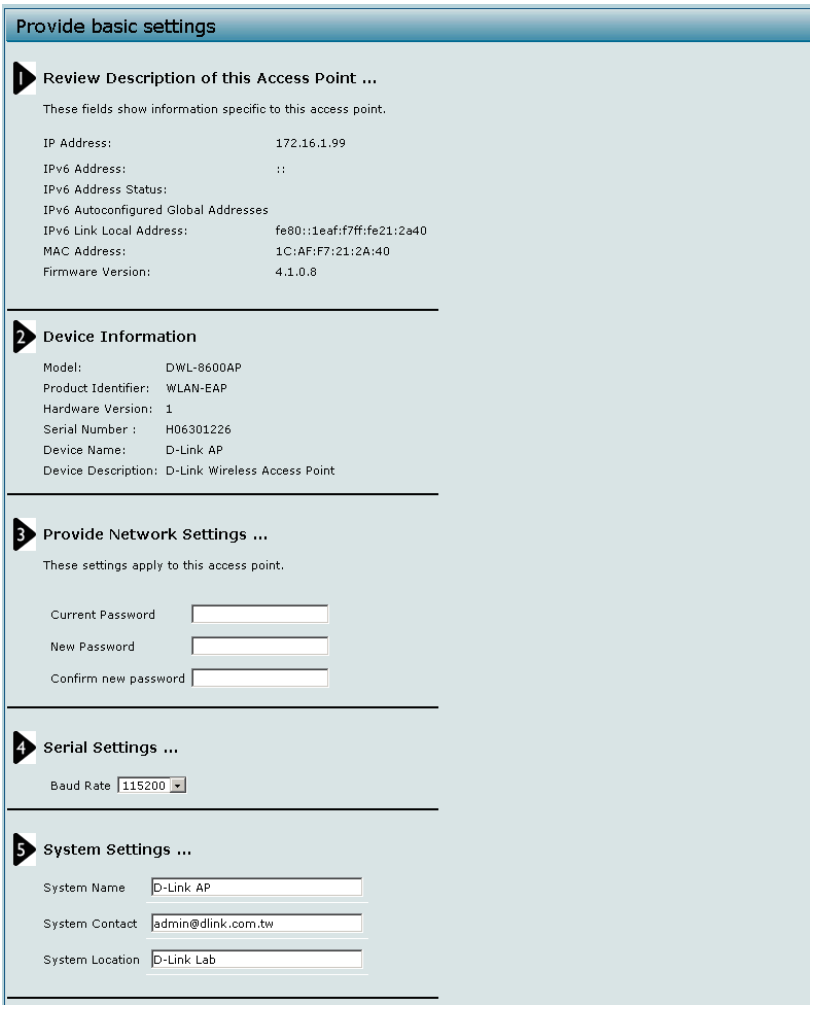


図 3-7　Basic Settings 画面

本画面には、**Basic Settings** メニューをクリックするか、**Tools > Basic Settings** の順にメニューをクリックして接続することもできます。

1. 「Provide basic settings」画面の設定を確認します。
アクセスポイントの詳細を確認し、パスワードの初期値「admin」を使用しない場合は、新しい管理者用パスワードを設定します。
「Apply」ボタンをクリックして、無線ネットワークの新しい設定を有効にします。

注意 変更を行ったら、「Apply」ボタンをクリックして設定を保存、および適用します。アクセスポイントの設定変更によっては、アクセスポイントのシステム停止、または再起動を引き起こすことがあります。この時、無線クライアントは一時的に接続を喪失します。アクセスポイントの設定変更は、WLAN トラフィックが低い時に行うことをお勧めします。

2. ご使用のネットワークに DHCP サーバが存在しない場合や使用する予定がない場合は、必ず接続タイプを「DHCP」から「Static IP」に変更してください。

アクセスポイントには、新しいスタティック IP アドレスの割り当ての実施、またはアドレスの初期値をそのまま使用することも可能です。しかし、同じネットワーク上に別の WLAN アクセスポイントを導入する場合には、各アクセスポイントの IP アドレスが異なるものになるように、新しいスタティック IP アドレスを割り当てることをお勧めします。接続タイプの変更およびスタティック IP アドレスの割り当てについては、「CLI を使用した IP アドレスの参照」（33 ページ）または、「Ethernet Settings（イーサネット設定）」（55 ページ）を参照してください。

3. ネットワークで VLAN を使用する場合、管理 VLAN ID またはタグなし VLAN ID を本製品に設定して、ネットワーク上で動作するようにする必要があります。VLAN の設定方法に関する詳細は、「CLI を使用した IP アドレスの参照」（33 ページ）または、「Ethernet Settings（イーサネット設定）」（55 ページ）を参照してください。

4. IEEE 802.1X のポートベースセキュリティでネットワークアクセス制御を利用するネットワークでは、必ず本製品に 802.1X サプリカント情報を設定してください。802.1X 認証のユーザ名やパスワードの設定方法に関する詳細は、「Authentication（802.1X 認証の設定）」（83 ページ）を参照してください。

以下の表では、「Provide Basic Settings」画面の各項目について説明します。

項目	説明
Review Description of this Access Point ...	
IP Address	本製品に割り当てられた IP アドレスを表示します。IP アドレスは、既に DHCP、または「Ethernet Settings（イーサネット設定）」画面でスタティックに割り当てられているので、本画面では変更できません。
IPv6 Address	本製品に割り当てられている IPv6 アドレスを表示します。IP アドレスは、既に DHCPv6、または「Ethernet Settings」画面でスタティックに割り当てられているので、本画面では変更できません。
IPv6 Address Status	AP の管理インタフェースとして設定されたスタティック IPv6 アドレスの状態を表示します。 「Operational」：管理中、「Tentative」：試験状態
IPv6 Autoconfigured Global Addresses	AP の管理インタフェースとして自動的に設定されたグローバル IPv6 アドレスを表示します。
IPv6 Link Local Address	ローカルの物理的なリンクによって使用される IPv6 リンクローカルアドレスを表示します。リンクローカルアドレスは、IPv6 Neighbor 探索プロセスを使用して割り当てられるため、変更はできません。
MAC Address	本製品の MAC アドレスを表示します。ここに表示されるアドレスは、管理インタフェースに接続している MAC アドレスになります。外部の他のネットワークに対する本製品のアドレスになります。
Firmware Version	本製品にインストールされている現在ファームウェアのバージョン情報を表示します。WLAN アクセスポイントファームウェアの最新バージョンが利用可能になった場合、アップグレードすることができます。
Device Information	
Product Identifier	アクセスポイントのハードウェアモデル。
Hardware Version	アクセスポイントのハードウェアバージョン。
Serial Number	アクセスポイントのシリアル番号。
Device Name	ハードウェアのタイプを識別する一般名。
Device Description	製品ハードウェア情報。
Provide Network Settings ...	
Current Password	現在の管理者パスワードを入力します。変更する前に現在のパスワードを正確に入力してください。
New Password	新しい管理者パスワードを入力します。入力時に周囲から見られないように、入力した英数字は「 * 」で表示されます。管理者パスワードは 8 文字以内の半角英数字で入力します。記号やスペースは使用できません。 **注意** 無線ネットワークのセキュリティ性を確保する第一ステップとして、管理者パスワードを初期値から直ちに変更することをお勧めします。
Confirm new password	新しい管理者パスワードを確認のために再度入力します。
Serial Settings ...	
Baud Rate	シリアルポート接続のボーレートを指定します。本製品のボーレートは、シリアル接続を使用して本製品の CLI に接続しているターミナルまたはターミナルエミュレータのボーレートと必ず一致させてください。 使用できるボーレートは以下の通りです。 • 9600 • 19200 • 38400 • 57600 • 115200（初期値）
System Settings ...	
System Name	本製品の名称を入力します。この名前はここでだけ表示されるもので、管理者が本製品を識別するための名称です。64 文字までの半角英数字を入力します。（例：My AP）
System Contact	本製品に関連する問題などの問い合わせ先の名前、E-mail アドレス、電話番号を入力します。
System Location	本製品の設置場所を入力します。（例：Conference Room A）

IPV6 アドレスを使用して本製品の Web インタフェースに接続する

IPv6 グローバルアドレスまたは IPv6 リンクローカルアドレスを使用して本製品に接続するためには、本製品のアドレスを特別な形式で Web ブラウザに入力する必要があります。

注意 以下の手順および例題は、Microsoft Internet Explorer 7（IE7）を使用した場合のものであり、他のブラウザでは動作しないことがあります。

- IPv6 グローバルアドレスに接続するためには、IPv6 アドレスの前後に角括弧 [ ] を入力します。例えば、アクセスポイントの IPv6 グローバルアドレスが「2520::230:abff:fe00:2420」であれば、アドレスバーに以下のように入力します。
  http://[2520::230:abff:fe00:2420]

- IPv6 リンクローカルアドレスに接続するためには、コロン（:）をハイフン（-）に置き換え、インタフェース番号の前に「s」を付けたものを追加し、「.ipv6-literal.net」を入力します。例えばアクセスポイントのリンクローカルアドレスが「fe80::230abff:fe00:2420」、Windows のインタフェースが「%6」で定義される場合は、アドレスバーに以下のように入力します。
  http://fe80--230-abff-fe00-2420s6.ipv6literal.net

Web マネージャのメニュー構成

Web マネージャで本製品に接続し、ログイン画面でユーザ名とパスワードを入力して本製品の管理モードにアクセスします。
Web マネージャで設定可能な機能は次ページで説明します。

メインメニュー	サブメニュー	説明	参照ページ
Basic Settings	—	IP/MAC アドレス情報などの情報の参照、および管理者パスワードの設定を行います。	30 ページ
Status	Interfaces	イーサネット LAN および無線 LAN（WLAN）設定をモニタリングします。	39 ページ
	Events	システムイベントをリアルタイムで表示します。	40 ページ
	Transmit/Receive	インタフェース上の VAP で送受信するデータの統計情報をリアルタイムで表示します。	43 ページ
	Client Associations	特定のアクセスポイントに接続するクライアントステーションを参照します。	45 ページ
	TSPEC Client Associations	アクセスポイントに接続する TSPEC クライアントステーションを参照します。	46 ページ
	Rogue AP Detection	Web マネージャ画面で参照しているアクセスポイント範囲にあるすべてのアクセスポイントのリアルタイム統計情報を提供します。	47 ページ
	Managed AP DHCP	DHCP サーバから学習した D-Link 統合スイッチの DNS 名または IP アドレスを表示します。	50 ページ
	TSPEC Status and Statistics	TSPEC セッションの要約情報、TSPEC VAP のリアルタイム送受信統計情報について表示します。	50 ページ
	TSPEC AP Statistics	「TSPEC AP Statistics」TSPEC AP 統計情報のページでは AP によって許可 / 破棄された音声 / 映像トラフィックストリームの情報について表示します。	51 ページ
	Radio Statistics	「Radio Statistics」ページでは本アクセスポイントで送受信されたパケット / バイトについての詳しい情報を表示します。	52 ページ
	Email Alert Status	「Email Alert Operational Status」はアクセスポイントで起動しているシスログメッセージを基本にした E メールアラートです。	53 ページ
Manage	Ethernet Settings	本製品の LAN インタフェースを設定します。	55 ページ
	Wireless Settings	本製品の無線インタフェースに基本的な設定します。	57 ページ
	Radio	本製品の無線インタフェースに詳細な設定を行います。	59 ページ
	Scheduler	無線と VAP のスケジューラ設定はスタンドアロン利用時の機能です。	63 ページ
	Scheduler Association	スケジューラプロファイルを設定・有効にします。	65 ページ
	VAP	仮想アクセスポイントの設定を行います。	66 ページ
	WDS	WDS の設定を行います。	74 ページ
	MAC Authentication	無線クライアントの MAC アドレスに基づいてアクセスポイント経由でネットワークへのアクセスを制御します。	78 ページ
	Load Balancing	ロードバランシングの設定を行います。	80 ページ
	Managed Access Point	管理アクセスポイントの設定を行います。	81 ページ
	Authentication	802.1X サプリカントのユーザ名とパスワードを設定します。	83 ページ
	Management ACL	アクセスコントロールリスト（ACL）を作成します。	84 ページ
Services	Web Server	Web サーバの設定を行います。	85 ページ
	SNMP	SNMPv1 、SNMPv2c の設定を行います。	87 ページ
	SSH	SSH アクセスを有効または無効にします。	89 ページ
	Telnet	Telnet アクセスを有効または無効にします。	89 ページ
	QoS	QoS の設定を行います。	90 ページ
	Email Alert	「Email Alert」機能は幾つかのレベル分けされたイベントによって AP が自動的に E メールを送信する機能です。	92 ページ
	Time Settings	NTP を使用してクロックタイムを同期させます。	94 ページ
SNMPv3	SNMPv3 Views	SNMPv3 ユーザがアクセスできる OID 範囲を制御するために MIB ビューを作成します。	95 ページ
	SNMPv3 Groups	異なる許可とアクセス権を持つ SNMPv3 グループを設定します。	96 ページ
	SNMPv3 Users	各ユーザにセキュリティレベルを設定します。	97 ページ
	SNMPv3 Targets	SNMPv3 ターゲットの設定を行います。	98 ページ
Maintenance	Configuration Save	現在のコンフィグレーションファイルを保存します。	99 ページ
	Configuration Restore	保存したコンフィグレーションをリストアします。	101 ページ
	Maintenance	本製品の工場出荷時設定へのリセット、および再起動を行います。	103 ページ
	Upgrade	ファームウェアを最新バージョンに更新します。	104 ページ
	Packet Capture	無線パケットキャプチャについて二つのモードで設定します。	106 ページ

メインメニュー	サブメニュー	説明	参照ページ
Client QoS	VAP QoS Parameters	ネットワークに接続する無線クライアントの QoS に個々のクライアントが送受信を許可される帯域幅のコントロールを行います。	112 ページ
	Managing Client QoS ACL	IPv4 アクセスコントロールリストを設定します。	113 ページ
	Class Map	DiffServ クラスマップを作成します。	120 ページ
	Policy Map	Diffserv ポリシーマップを作成します。	125 ページ
	Client QoS Status	現在アクセスポイント接続している各クライアントに適用されるクライアント QoS 設定を表示します。	127 ページ
	Configuring RADIUS-Assigned Client QoS Parameters	クライアントの RADIUS サーバエントリに含むことのできる QoS 属性にについて説明します。	127 ページ
Cluster	Access Points	クラスタメンバの参照と設定を行います。	129 ページ
	Sessions	クラスタ内のアクセスポイントに接続するクライアントステーションの情報を表示します。	132 ページ
	Channel Management	クラスタメンバにチャンネル割り当ての設定、または参照を行います。	133 ページ
	Wireless Neighborhood	Neighbor アクセスポイントの無線インタフェースの統計情報と識別情報を表示します。	136 ページ

コンソールポートを使用した管理

CLI を使用した IP アドレスの参照

本製品の DHCP クライアント機能は、初期値で有効です。本製品を DHCP サーバが存在するネットワークに接続すると、自動的に IP アドレスを取得します。管理者ユーザインタフェースを使用して本製品を管理するためには、必ず本製品の IP アドレスを Web ブラウザに入力してください。

コンソールポートを使用したネットワーク情報の設定は、以下の手順で行います。

1. モデムケーブルを使用して、VT100/ANSI 端末かワークステーションをコンソール（シリアル）ポートに接続します。
PC、Apple や UNIX のワークステーションと接続する場合は、ハイパーターミナルなどの端末エミュレーションプログラムを起動してください。

2. 端末エミュレーションプログラムの設定を以下に合わせてください。
- データ速度 : 115,200bps
- データビット : 8
- パリティ : なし
- ストップビット : 1
- フロー制御 : なし

3. 「Enter」キーを押すとログインプロンプトが表示されます。
ユーザ名に「**admin**」と入力してください。パスワードの初期値は「**admin**」です。

ログインに成功すると、画面のプロンプトが 「DLINK-WLAN-AP #」に変わります。

図 3-8　ログイン成功画面（CLI）

4. プロンプトが表示されたら、「get management」と入力します。
以下の画面が表示されます。

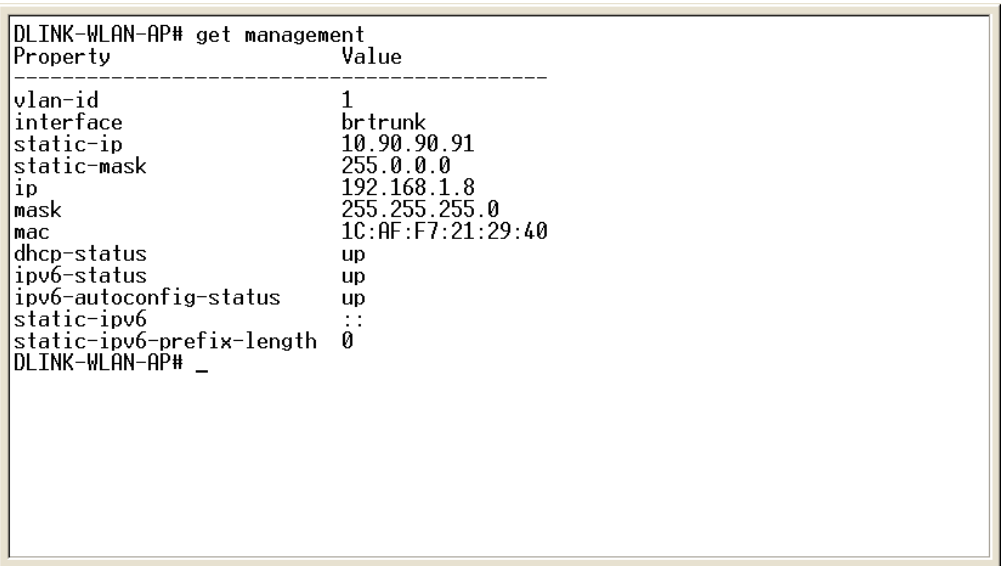


図 3-9　get management 画面（CLI）

イーサネット設定

DHCP および VLAN 情報を含むイーサネットの初期設定では、動作しないネットワークがある可能性があります。

初期設定では、本製品の DHCP クライアントが自動的にネットワーク情報のリクエストをブロードキャストします。スタティック IP アドレスを使用したい場合は、DHCP クライアントを無効にして、手動で IP アドレスとその他のネットワーク情報を設定する必要があります。

管理用 VLAN は、初期値で「VLAN 1」に指定されています。本 VLAN は初期値でタグなしの VLAN です。ネットワーク上に異なる VLAN ID を使用した管理用 VLAN が存在している場合は、本製品の管理用 VLAN の VLAN ID を変更する必要があります。

Web インタフェースを使用するイーサネット設定についての詳細は、「Ethernet Settings（イーサネット設定）」（55 ページ）を参照してください。次のセクションで説明するように、CLI を使用してイーサネット設定を行うこともできます。

CLI を使用したイーサネット設定

以下の表のコマンドを使用してイーサネット（有線）インタフェースの値を参照および設定します。

各設定に関する詳細は、以下の通りです。

アクション	コマンド
DNS 名を確認する	get host id
DNS 名を設定する	set host id <host_name> 例：set host id vicky-ap
イーサネット（有線）内部インタフェースの現在の設定を確認する	get management
管理 VLAN ID を設定する	set management vlan-id <1-4094>
タグなし VLAN 情報を参照する	get untagged-vlan
タグなし VLAN を有効にする	set untagged-vlan status up
タグなし VLAN を無効にする	set untagged-vlan status down
タグなし VLAN ID を設定する	set untagged-vlan vlan-id <1-4094>
接続タイプを参照する	get management dhcp-status
DHCP を接続タイプとして使用する	set dhcp-client status up
スタティック IP を接続タイプとして使用する	set dhcp-client status down
スタティック IP アドレスを設定する	set management static-ip <ip_address> 例：set management static-ip 10.10.12.221
サブネットマスクを設定する	set management static-mask <netmask> 例：set management static-mask 255.255.255.0
デフォルトゲートウェイを設定する	set static-ip-route gateway <ip_address> 例：set static-ip-route gateway 10.10.12.1
DNS ネームサーバモード（Dynamic= up Manual=down）を参照する	get host dns-via-dhcp
DNS ネームサーバにスタティックな IP アドレスを使用するように設定する（ダイナミックモードから手動モードへの変更）	set host dns-via-dhcp down set host static-dns-1 <ip_address> set host static-dns-2 <ip_address> 例：set host static-dns-1 192.168.23.45
DNS ネームサーバに DHCP により割り振られる IP アドレスを使用するように設定する（手動モードからダイナミックモードへの変更）	set host dns-via-dhcp up

以下の例では、管理者が CLI を使用して、管理用 VLAN ID を「123」に設定し、すべてのトラフィックがタグ付けされて VLAN ID を持つように、タグなし VLAN を無効にします。

```
DLINK-WLAN-AP# set management vlan-id 123
dman: Restarting DHCP client
DLINK-WLAN-AP# set untagged-vlan status down
dman: Restarting DHCP client

DLINK-WLAN-AP# get management
Property                  Value
----------------------------------------
vlan-id                   123
interface                 brtrunk
static-ip                 10.90.90.91
static-mask               255.0.0.0
ip                        192.168.1.8
mask                      255.255.255.0
mac                       1C:AF:F7:21:29:40
dhcp-status               up
ipv6-status               up
ipv6-autoconfig-status    up
static-ipv6               ::
static-ipv6-prefix-length  0
DLINK-WLAN-AP#
DLINK-WLAN-AP# get untagged-vlan
Property  Value
---------------
vlan-id   1
status    down

DLINK-WLAN-AP#
```

IEEE 802.1X 認証の設定

IEEE 802.1X ポートベースのネットワークアクセス制御を利用するネットワークでは、サプリカント（クライアント）は 802.1X オーセンティケータにアクセスが許可されるまで、ネットワークへアクセスすることができません。ネットワークで 802.1X 認証が使用されている場合は、アクセスポイントに 802.1X 認証情報を登録する必要があります。

ご使用のネットワークが IEEE 802.1X を使用している場合、Web インタフェースを使用した 802.1X 認証の設定方法に関する詳細は、「Authentication（802.1X 認証の設定）」（83 ページ）を参照してください。

CLI を使用した 802.1X 認証の設定

802.1X サプリカント情報の設定に使用する CLI コマンドを以下の通りです。

アクション	コマンド
802.1X サプリカント設定を表示する	get dot1x-supplicant
802.1X サプリカントを有効にする	set dot1x-supplicant status up
802.1X サプリカントを無効にする	set dot1x-supplicant status down
802.1X ユーザ名を設定する	set dot1x-supplicant user <name>
802.1X ユーザのパスワードを設定する	set dot1x-supplicant password <password>

以下の例では、管理者が 802.1X サプリカント機能を有効にし、ユーザ名を「wlanAP」、パスワードを「test1234」に登録します。

```
DLINK-WLAN-AP# set dot1x-supplicant status up
DLINK-WLAN-AP# set dot1x-supplicant user wlanAP
DLINK-WLAN-AP# set dot1x-supplicant password test1234
DLINK-WLAN-AP# get dot1x-supplicant
Property  Value
----------------
status    up
user      wlanAP
DLINK-WLAN-AP#
```

インストールの確認

本製品が LAN に接続し、ネットワークに無線クライアントが接続していることを確認してください。無線ネットワークの基本設定を確認した後、詳細設定を行うことで、さらにセキュリティ性の高い詳細な設定を行うことができるようになります。

1. 本製品を LAN に接続します。
   本製品および管理者用コンピュータを 1 つのハブに接続している場合、本製品は既に LAN に接続しています。次に無線クライアントのテストを行います。

   本製品を直接ケーブルでご使用のコンピュータに接続している場合は、以下の手順で行います。
   - 本製品とコンピュータのケーブルを外します。
   - 本製品をイーサネットケーブルで LAN に接続します。
   - イーサネットケーブルまたは無線 LAN カードを使用して、コンピュータを LAN に接続します。

2. 無線クライアントと LAN の接続を確認します。
   無線クライアントデバイスから、本製品を検出して接続することで本製品を確認します。無線クライアントの必要環境については、「無線クライアントの必要環境」（19 ページ）を参照してください。

3. 詳細設定により、本製品にセキュリティ設定をします。
   無線ネットワークが動作し、本製品が無線クライアントに接続した後に、セキュリティレイヤの追加、複数の VAP の作成、および性能設定を行うことができます。

注意 WLAN アクセスポイントには、同時に複数の設定変更を行うことはできません。1 人以上の管理者が管理者用 Web 画面にログインし、設定変更を行う場合、複数のユーザによって指定された設定の変更が適用される保証はありません。

初期設定では、本製品にはセキュリティ設定は行われていないため、どの無線クライアントからもアクセスポイントやご使用のネットワーク に接続することができます。次に重要な手順は、セキュリティの設定を行うことです。これは、「VAP（仮想アクセスポイントの設定）」（66 ページ）で説明します。

無線アクセスポイントのセキュリティ設定

有効な各仮想アクセスポイント（VAP）にセキュリティ設定を行い、セキュアな無線クライアントを設定します。1 つの物理アクセスポイントで、最大 16 個の VAP を設定して複数のアクセスポイントのように設定することができます。初期値では、有効な VAP は 1 つです。各 VAP に異なるセキュリティモードを設定して無線クライアントの接続を制御することができます。

それぞれの無線機器には VAP ID が 0-15 の 16 個の VAP があります。初期値では、VAP 0 のみ有効です。
VAP 0 の初期設定は以下の通りです。

- VLAN ID：1
- Broadcast SSID：有効
- SSID：dlink1
- Security：なし
- MAC Authentication Type：なし
- Redirect Mode：なし

他のすべての VAP は初期値で無効です。VAP 1-15 の SSID の初期値 は、dlinkx（x は VAP ID）になります。

本製品への不正アクセスを防止するために、VAP の初期値および有効にした各 VAP のセキュリティオプションで「None」以外を選択して変更を行うことをお勧めします。

各 VAP のセキュリティ設定方法に関する詳細は、「VAP（仮想アクセスポイントの設定）」（66 ページ）を参照してください。

第 4 章　Status（アクセスポイントステータスの参照）

本セクションではメインメニューの「Status」の各サブメニューから参照可能な情報について説明します。

設定項目	説明	参照ページ
Interfaces（インタフェースステータスの参照）	イーサネット LAN および無線 LAN（WLAN）設定をモニタリングします。	39 ページ
Events（イベントの参照）	システムイベントをリアルタイムで表示します。	40 ページ
Transmit/Receive（送受信した統計情報の参照）	インタフェース上の VAP で送受信するデータの統計情報をリアルタイムで表示します。	43 ページ
Client Associations （接続する無線クライアント情報の参照）	特定のアクセスポイントに接続するクライアントステーションを参照します。	45 ページ
TSPEC Client Associations （TSPEC クライアント情報の参照）	アクセスポイントに接続する TSPEC クライアントステーションを参照します。	46 ページ
Rogue AP Detection （不正アクセスポイントの検出）	Web マネージャ画面で参照しているアクセスポイント範囲にあるすべてのアクセスポイントのリアルタイム統計情報を提供します。	47 ページ
Managed AP DHCP （管理アクセスポイントの DHCP 情報の表示）	DHCP サーバから学習した D-Link 統合スイッチの DNS 名または IP アドレスを表示します。	50 ページ
TSPEC Status and Statistics （TSPEC ステータスと統計情報の参照）	「TSPEC Status and Statistics」ページでは、「無線による TSPEC セッションの要約情報」「VAP による TSPEC セッションの要約情報」「全ての無線インタフェースの TSPEC VAP のリアルタイム送受信統計情報」について表示します。	50 ページ
TSPEC AP Statistics（TSPEC AP 統計情報の参照）	TSPEC AP 統計情報のページでは AP によって許可 / 破棄された音声 / 映像トラフィックストリームの情報について表示します。	51 ページ
Radio Statistics（無線統計情報の参照）	本アクセスポイントで送受信されたパケット / バイトについての詳しい情報を表示します。	52 ページ
Email Alert Status （E メールアラートステータスの参照）	アクセスポイントで起動しているシスログメッセージを基本にした E メールアラートの設定です。	53 ページ

注意　本マニュアルでは、WEB GUI の画面として DWL-8600AP のものを使用しています。DWL-2600AP/3600AP/6600AP の WEB GUI 画面と一部差異がある場合がありますが、ご了承ください。

Interfaces（インタフェースステータスの参照）

イーサネット LAN および無線 LAN（WLAN）設定を参照します。

Status > Interfaces の順にメニューをクリックし、以下の画面を表示します。

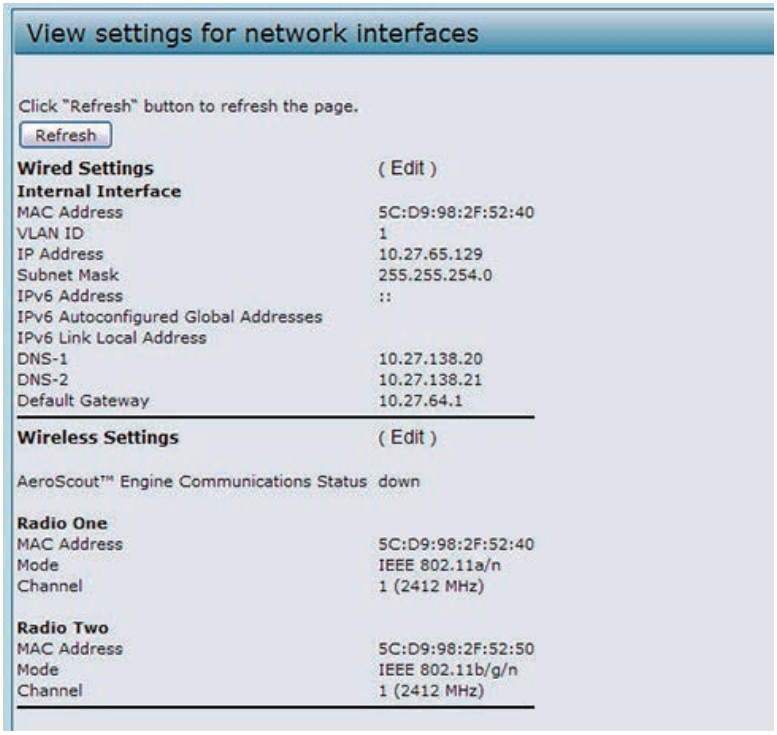


図 4-1　ネットワークインタフェースの設定参照 画面

本画面では現在の本製品の設定を表示します。「Wired Settings」（有線設定）と「Wireless Settings」（無線設定）を表示します。

Wired Settings（有線設定）（内部インタフェース）

内部インタフェースには、イーサネット MAC アドレス、管理 VLAN ID、IP アドレス（IPv4 および IPv6）、サブネットマスク、および DNS 情報があります。これらの設定を変更する場合は、「Edit」リンクをクリックし、「Modify Ethernet (Wired) settings」画面を表示します。

これらの設定項目については、「Ethernet Settings（イーサネット設定）」（55 ページ）を参照してください。

Wireless Settings（無線設定）

無線インタフェースには無線モードとチャンネルがあります。ここでは、各無線インタフェースに関連する MAC アドレス（参照のみ）も表示します。

無線の「Mode」または「Channel」を変更する場合には、「Edit」リンクをクリックし、無線設定画面を表示します。

これらの設定項目については、「Wireless Settings（無線設定）」（57 ページ）および「Radio（無線の詳細設定）」（59 ページ）を参照してください。

Events（イベントの参照）

アクセスポイントへの無線クライアントの接続や認証などアクセスポイントに発生するシステムイベントをリアルタイムで表示します。

システムイベントを参照するためには、**Status > Events** の順にメニューをクリックし、以下の画面を表示します。

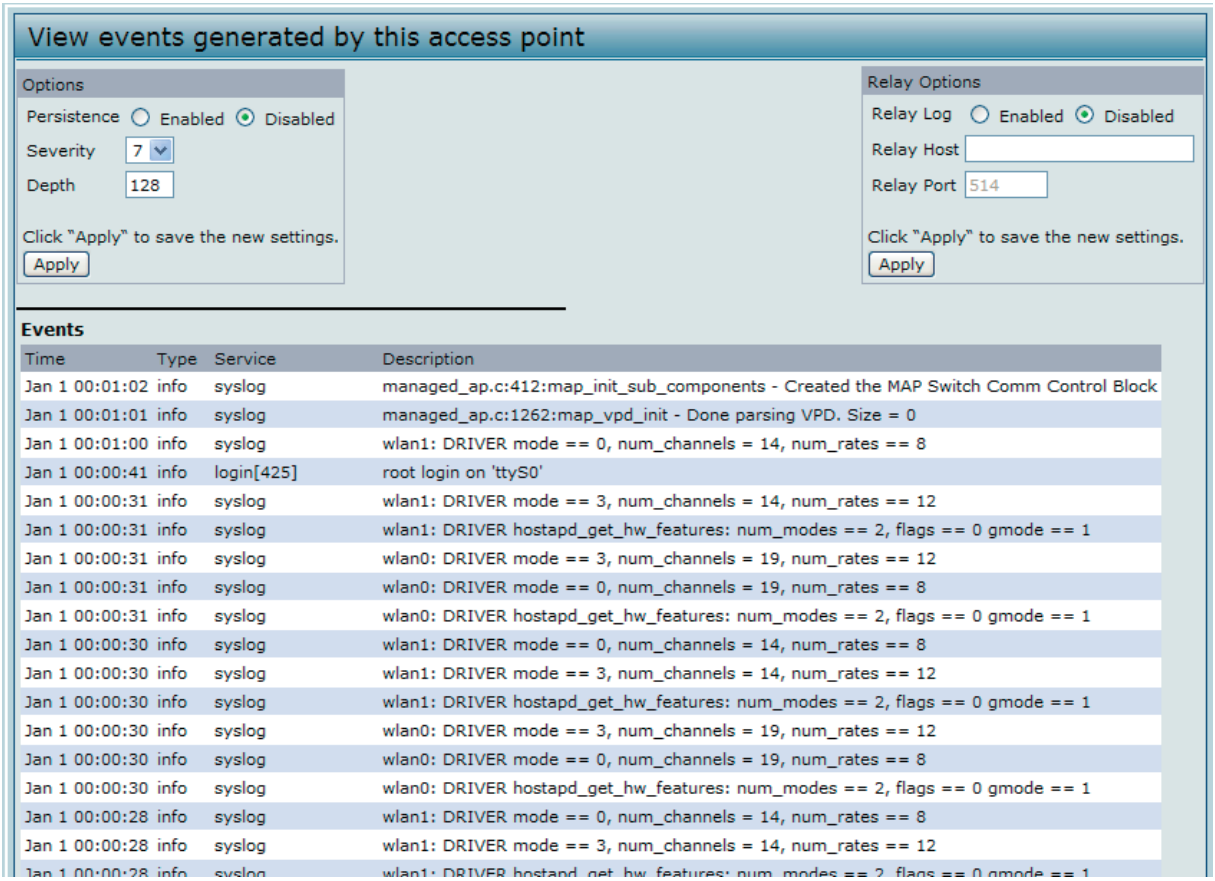


図 4-2　アクセスポイントが生成したイベントの参照 画面

本画面では、このアクセスポイントが生成した最新のイベントの参照およびログへの出力設定を行うことができます。システムの再起動時にイベントが消去されないように不揮発性メモリにシステムイベントログを出力する持続性ログ出力機能を有効および設定することができます。本画面では、リモートログリレーホストが Kernel Log 内のすべてのシステムイベントとエラーを取得できるオプションを提供します。

注意　本アクセスポイントは、ネットワークタイムプロトコル（NTP）を使用して日付と時間情報を取得します。このデータは UTC 形式（グリニッジ標準時として知られる）で通知されます。通知時間を使用する場所の時間に変換する必要があります。ネットワークタイムプロトコル設定に関する情報については、「Time（NTP サーバの有効化）」（94 ページ）を参照してください。

Options（持続性ログオプションの設定）

システムが予期せずに再起動する場合、ログメッセージは、その原因を分析するために有効です。しかし、持続性ログ出力を有効にしないと、システムの再起動時に、ログメッセージは削除されてしまいます。

警告 持続性ログの取得を有効にすると、フラッシュ（不揮発性）メモリが消耗して、ネットワーク性能は低下する可能性があります。問題をデバッグする場合にだけ、持続性のログ出力を有効にする必要があります。問題のデバッグの終了後に持続性のログ出力を必ず無効にします。

持続性ログを設定するためには、以下の図で記述されているように「Persistence」、「Severity」、および「Depth」オプションを設定して「Apply」ボタンをクリックします。

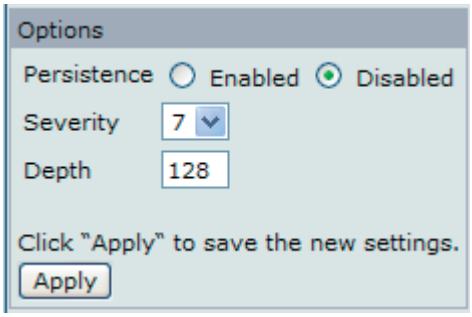


図 4-3　ログオプション画面

項目	説明
Persistence	• Enabled - アクセスポイントの再起動時にログを削除しないように不揮発性メモリにログを保存します。 • Disabled - 揮発性メモリにシステムログを保存します。揮発性メモリ内のログは、システムの再起動時に削除されます。
Severity	不揮発性メモリに記載するログメッセージの重要度レベルを指定します。例えば、2 を指定すると、critical、alert、および emergency ログが不揮発性メモリに記載され、3-7 の重要度レベルを持つエラーメッセージが揮発性メモリに出力されます。 • 0 - emergency • 1 - alert • 2 - critical • 3 - error • 4 - warning • 5 - notice • 6 - info • 7 - debug
Depth	不揮発性メモリには最大 128 個のメッセージを保存することができます。この領域内に設定した数値に到達すると、最も古いログイベントは新しいログイベントに書き換えられます。

注意 変更を適用するためには「Apply」ボタンをクリックします。設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

Relay Options（カーネルメッセージ用のログリレーホストの設定）

カーネルログはシステムログ内に記載されるシステムイベントやフレームの破棄のようなエラー状態を含むカーネルメッセージを持つ総合的なリストです。

Web マネージャを使用してアクセスポイントに対して直接カーネルログメッセージを参照することはできません。はじめに Syslog プロセスが動作し、ご使用のネットワークで Syslog のログリレーホストとして動作するリモートサーバを設定します。その後、リモートサーバに Syslog メッセージを送信するように本製品を設定することができます。

アクセスポイントの Syslog メッセージをリモートログサーバが収集することで、以下の機能を提供します。

- 複数のアクセスポイントから Syslog メッセージの収集を行うことができます。
- 単一のアクセスポイントで保持するメッセージよりも長いヒストリを保存することができます。
- スクリプト化された管理操作およびアラートを起動することができます。

カーネルログリレー機能を使用するためには、リモートサーバを設定して Syslog メッセージを受信する必要があります。リモートログホストを設定する手順は、リモートホストなどご使用のシステムタイプによって異なります。

注意 Syslog プロセスは、ポート 514 を初期値で使用します。このポートの初期値を使用することをお勧めします。しかし、ログポートを再設定する場合には、Syslog ポートに割り当てるポート番号が別のプロセスに使用されていないことをご確認ください。

ログリレーホストの有効 / 無効化

ログリレーの有効 / 無効化、および設定を行うためには、以下の表に示すログリレーオプションを設定して「Apply」ボタンをクリックします。

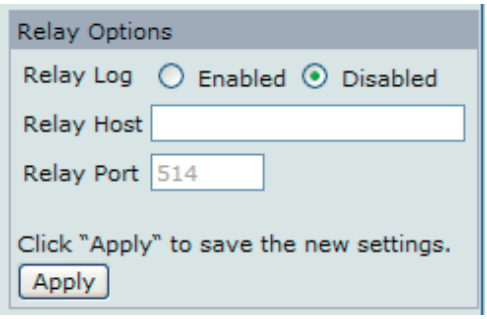


図 4-4　ログリレーホスト設定オプション画面

項目	説明
Relay Log	• Enabled - リモートホストへのログメッセージの送信を本製品に許可します。 • Disabled - すべてのログメッセージをローカルシステムに保持します。
Relay Host	リモートログサーバの IP アドレスまたは DNS 名を指定します。
Relay Port	リレーホストの Syslog プロセス用のポート番号を指定します。初期値は 514 です。

注意　変更を適用するためには「Apply」ボタンをクリックします。設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

ログリレーホストを「Enabled」（有効）にして「Apply」ボタンをクリックすることと、リモートログ出力がアクティブになります。アクセスポイントは、ログリレーホストを設定した方法により、リモートログサーバモニタ、定義したカーネルログファイル、または他のストレージに対して表示用のカーネルメッセージをリアルタイムに送信します。

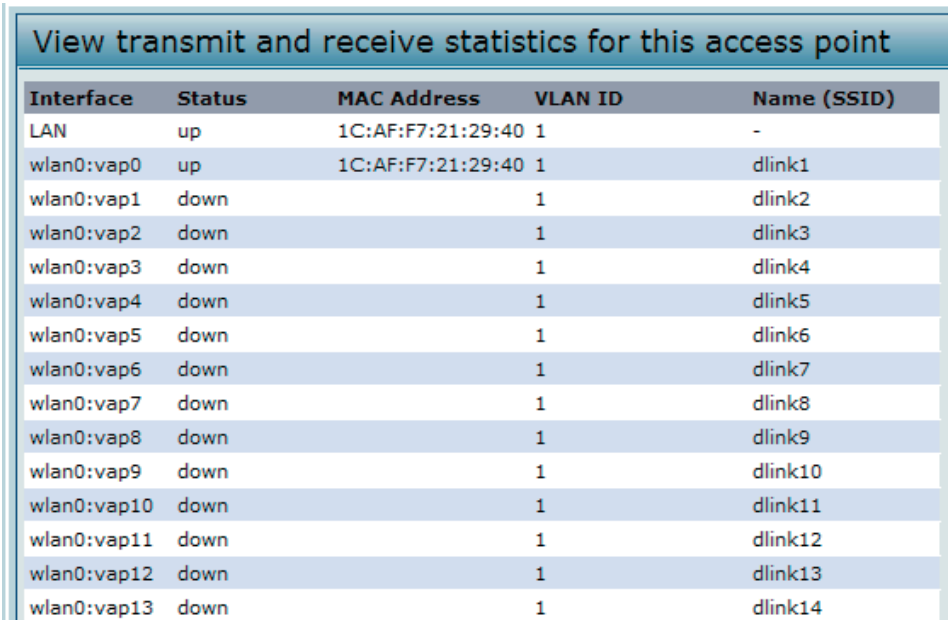
ログリレーホストを「Disabled」（無効）にして「Apply」ボタンをクリックすると、リモートログ出力は無効になります。

Transmit/Receive（送受信した統計情報の参照）

現在のアクセスポイントに関する基本的な情報とアクセスポイント上のイーサネットインタフェースおよび両無線インタフェース上の VAP で送受信するデータの統計情報をリアルタイムで表示します。参照される送受信データの統計情報のすべてが、アクセスポイントが最後に起動してからの合計です。アクセスポイントを再起動すると、これらの数字は、再起動後の送受信データの合計を示します。

アクセスポイントに送受信するデータの統計情報を参照します。

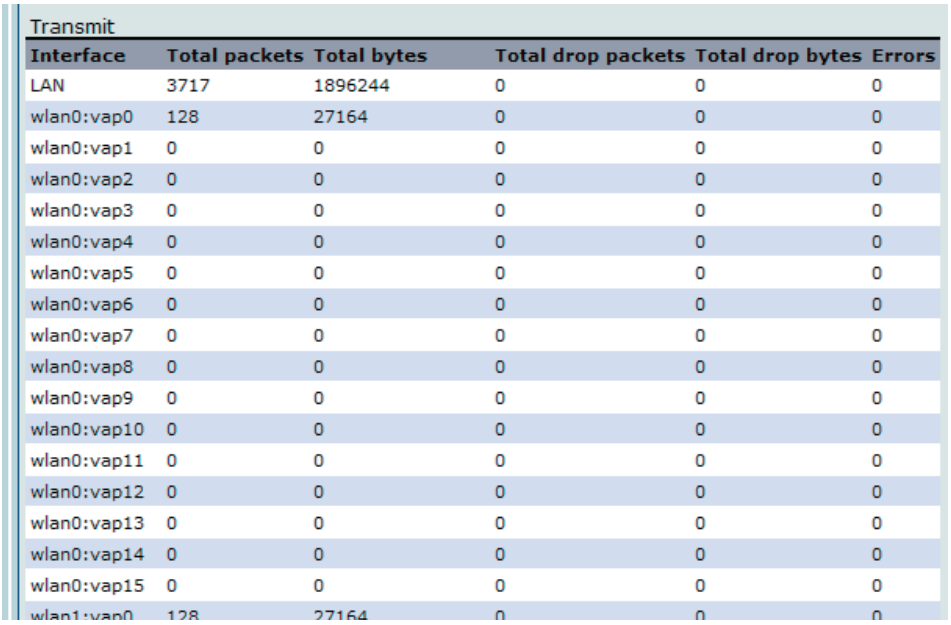
Status > Transmit/Receive の順にメニューをクリックし、以下の画面を表示します。



View transmit and receive statistics for this access point

Interface	Status	MAC Address	VLAN ID	Name (SSID)
LAN	up	1C:AF:F7:21:29:40	1	-
wlan0:vap0	up	1C:AF:F7:21:29:40	1	dlink1
wlan0:vap1	down		1	dlink2
wlan0:vap2	down		1	dlink3
wlan0:vap3	down		1	dlink4
wlan0:vap4	down		1	dlink5
wlan0:vap5	down		1	dlink6
wlan0:vap6	down		1	dlink7
wlan0:vap7	down		1	dlink8
wlan0:vap8	down		1	dlink9
wlan0:vap9	down		1	dlink10
wlan0:vap10	down		1	dlink11
wlan0:vap11	down		1	dlink12
wlan0:vap12	down		1	dlink13
wlan0:vap13	down		1	dlink14

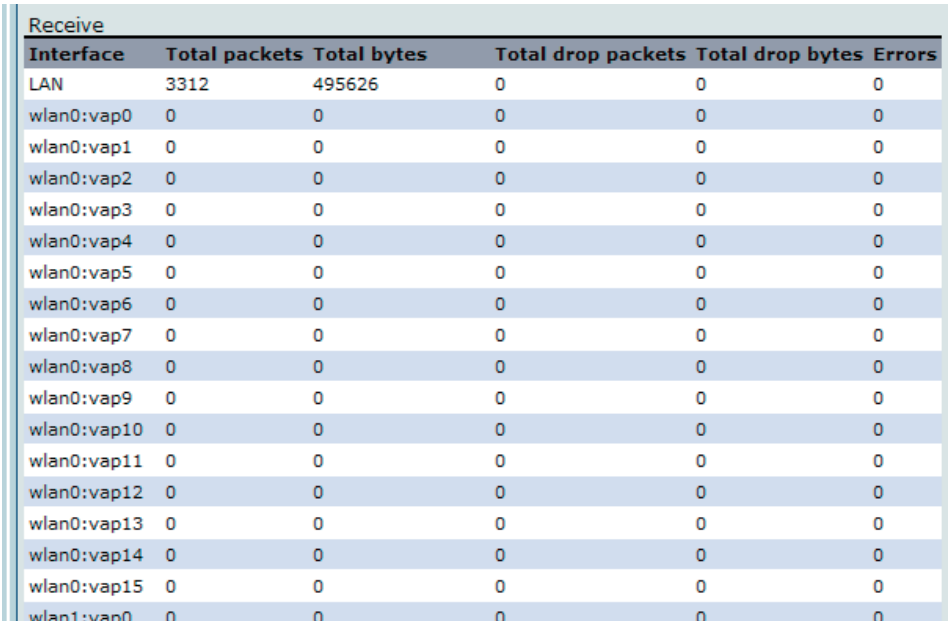
図 4-5　アクセスポイントの送受信トラフィックに関する統計情報の参照 画面



Transmit

Interface	Total packets	Total bytes	Total drop packets	Total drop bytes	Errors
LAN	3717	1896244	0	0	0
wlan0:vap0	128	27164	0	0	0
wlan0:vap1	0	0	0	0	0
wlan0:vap2	0	0	0	0	0
wlan0:vap3	0	0	0	0	0
wlan0:vap4	0	0	0	0	0
wlan0:vap5	0	0	0	0	0
wlan0:vap6	0	0	0	0	0
wlan0:vap7	0	0	0	0	0
wlan0:vap8	0	0	0	0	0
wlan0:vap9	0	0	0	0	0
wlan0:vap10	0	0	0	0	0
wlan0:vap11	0	0	0	0	0
wlan0:vap12	0	0	0	0	0
wlan0:vap13	0	0	0	0	0
wlan0:vap14	0	0	0	0	0
wlan0:vap15	0	0	0	0	0
wlan1:vap0	128	27164	0	0	0

図 4-6　トラフィック統計情報の参照画面 - Transmit



Receive

Interface	Total packets	Total bytes	Total drop packets	Total drop bytes	Errors
LAN	3312	495626	0	0	0
wlan0:vap0	0	0	0	0	0
wlan0:vap1	0	0	0	0	0
wlan0:vap2	0	0	0	0	0
wlan0:vap3	0	0	0	0	0
wlan0:vap4	0	0	0	0	0
wlan0:vap5	0	0	0	0	0
wlan0:vap6	0	0	0	0	0
wlan0:vap7	0	0	0	0	0
wlan0:vap8	0	0	0	0	0
wlan0:vap9	0	0	0	0	0
wlan0:vap10	0	0	0	0	0
wlan0:vap11	0	0	0	0	0
wlan0:vap12	0	0	0	0	0
wlan0:vap13	0	0	0	0	0
wlan0:vap14	0	0	0	0	0
wlan0:vap15	0	0	0	0	0
wlan1:vap0	0	0	0	0	0

図 4-7　トラフィック統計情報の参照画面 - Receive

以下の項目が表示されます。

項目	説明
Interface	イーサネットまたは VAP インタフェース名。
Status	インタフェースが「up」（アクティブ）または「down」（ダウン）かを表示します。
MAC Address	指定インタフェースの MAC アドレス。 本製品は、各インタフェースに対して固有の MAC ドレスを持っています。各無線インタフェースには、2 つの無線インタフェースに異なる MAC アドレスを持っています。（DWL-2600AP/3600AP は 1 つ）
VLAN ID	Virtual LAN（VLAN）ID。 VLAN を使用して、同じアクセスポイントに複数の内部ネットワークおよびゲストネットワークを確立することができます。VLAN ID は **Manage > VAP** メニューで設定されます。（「Load Balancing（ロードバランシングの設定）」（80 ページ）を参照してください。）
Name (SSID)	無線ネットワーク名。SSID として知られており、半角英数字で無線 LAN を識別します。 SSID は **Manage > VAP** メニューで設定されます。（「Load Balancing（ロードバランシングの設定）」（80 ページ）を参照してください。）
Transmit / Receive	
Total packets	本アクセスポイントが Transmit テーブルから送信したパケットまたは Received テーブルに受信したパケットの合計数を示します。
Total bytes	本アクセスポイントが Transmit テーブルから送信したパケットまたは Received テーブルに受信したバイト数の合計数を示します。
Total drop packets	本アクセスポイントが Transmit テーブルから送信したパケットまたは Received テーブルに受信し、破棄されたパケットの合計数を示します。
Total drop bytes	本アクセスポイントが Transmit テーブルから送信したパケットまたは Received テーブルに受信し、破棄されたバイト数の合計数を示します。
Errors	本アクセスポイントが送受信したデータに関連するエラーの合計数を示します。

Client Associations（接続する無線クライアント情報の参照）

アクセスポイントに接続するクライアントステーションを参照します。

Status > Client Associations の順にメニューをクリックし、以下の画面を表示します。

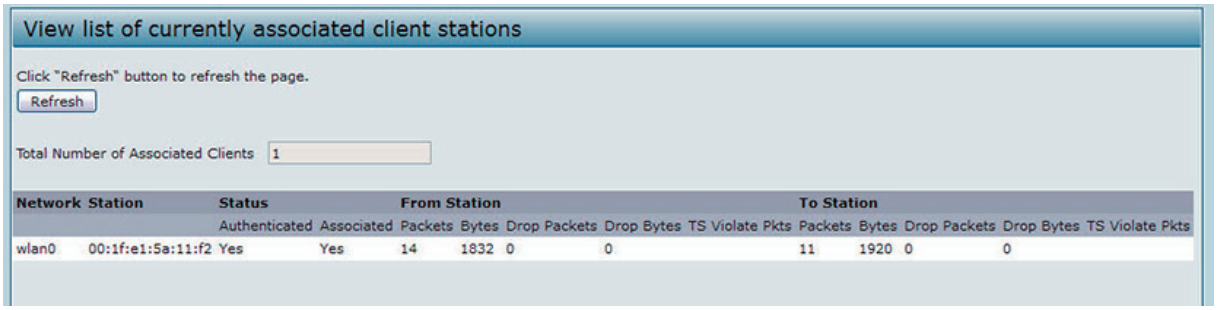


図 4-8　接続クライアントステーションリストの参照 画面

接続するステーションは、各ステーションが送受信したパケットトラフィックに関する情報と共に表示されます。

以下の表は、画面の各項目を説明します。

項目	説明
Network	クライアントが接続する VAP を表示します。例えば、wlan0vap2 のエントリは、クライアントが Radio 1 上の VAP2 に接続することを意味します。 wlan0 のエントリは、クライアントが Radio 1 上の VAP0 に接続することを意味します。wlan1 のエントリは、クライアントが Radio 2 の VAP0 に接続することを意味します。
Station	接続する無線クライアントの MAC アドレスを表示します。
Status	「Authenticated」および「Associated」ステータスは、基本的な IEEE 802.11 認証と接続ステータスを示しています。これは、クライアントがアクセスポイントに接続するのに使用するセキュリティのタイプがどれであっても存在するものです。このステータスは IEEE 802.1X の Authentication または Association ステータスを示すものではありません。 ここで注意すべき点は以下の通りです。 • アクセスポイントのセキュリティモードが「None」または「Static WEP」である場合、本画面で示すクライアントの「Authentication」および「Association」ステータスは、予期されるものに従います。つまり、クライアントがアクセスポイントに対して「authenticated」（認証済み）と示されると、データの送受信が可能になります。（これは、「Static WEP」が IEEE 802.11 認証だけを使用しているためです。） • しかし、アクセスポイントが、「IEEE 802.1X」または「WPA」セキュリティを使用すると、クライアントの接続がこのタブ上で（IEEE 802.11 セキュリティ経由で）認証されたものとして表示されますが、実際にはセキュリティの 2 番目のレイヤを通じてアクセスポイントに認証されていません。
From Station	無線クライアントから受信したパケットおよびバイト数と受信後に破棄されたパケットおよびバイト数を表示します。
To Station	アクセスポイントから送信されたパケットおよびバイト数と送信後に破棄されたパケットおよびバイト数を表示します。

TSPEC Client Associations（TSPEC クライアント情報の参照）

アクセスポイントに接続する TSPEC クライアントステーションを参照します。

「TSPEC Client Association」の状態と統計ページでは、TSPEC クライアントのリアルタイムでの送受信統計情報やクライアントのステータスなどの基本情報を表示します。 クライアントとしての動作が始まってから全ての送受信統計が表示されます。

TSPEC は QoS 有効な無線クライアントから AP にリクエストされた、トラフィックストリーム（TS）のためのネットワークアクセスの総量を指します。トラフィックストリームは、特定のユーザ優先度に属する無線クライアントによって識別されたデータパケットの集合体です。音声トラフィックストリーム一例として「Wi - Fi」認定電話からの音声優先トラフィックなどの CODEC 対応データパケットなどがあります。

ビデオトラフィックストリームの一例としては、企業サーバからのビデオ会議の提供を優先する無線ラップトップからの映像トラフィックなどが上げられます。TSPEC クライアントの統計情報については「TSPEC Client Associations」をクリックします。

Status > TSPEC Client Associations の順にメニューをクリックし、以下の画面を表示します。

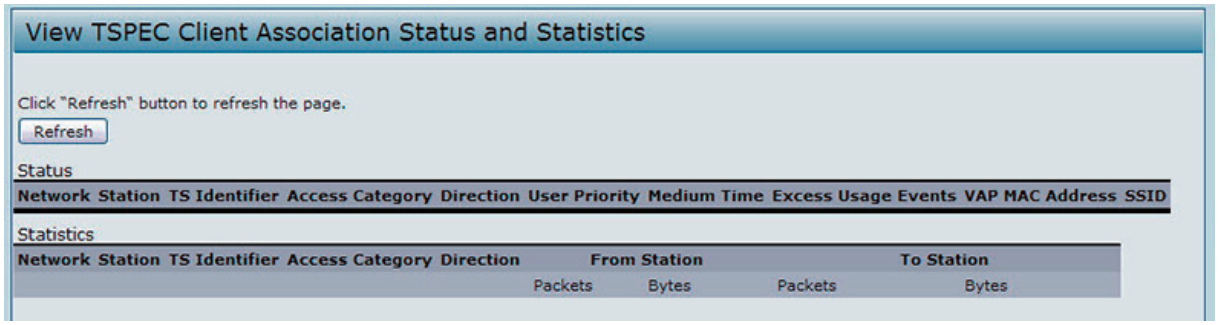


図 4-9　TSPEC クライアントステーションリストの参照 画面

接続するステーションは、各ステーションが送受信したパケットトラフィックに関する情報と共に表示されます。

以下の表は、画面の各項目を説明します。

項目	説明
Network	クライアントが接続する無線を表示します。
Station	接続する無線クライアントの MAC アドレスを表示します。
TS Identifier	TSPEC トラフィックセッションを識別します。(0 - 7)
Access Category	トラフィックストリームのアクセスカテゴリです。(音声 / 映像)
Direction	トラフィックストリームの方向性です。以下の 3 つがあります。 • uplink（アップリンク） • downlink（ダウンリンク） • bidirectional（双方向）
User Priority	トラフィックストリームのユーザ優先値（UP）です。UP は IP ヘッダの UP ポーションとして各パケットともに送信されます。 主な値は、 • 6 または 7（音声） • 4 または 5（映像） 他の優先トラフィックセッションにより数値は変動します。
Medium Time	このトラフィックストリームのクライアントに割り当てられた「Medium Time」(帯域)。クライアントにより提供 された TSPEC パラメータを使用する AP により、32μ 秒 / 秒単位で計測された値。
Excess Usage Events	クライアントが TSPEC に構成された「Medium Time」(帯域) を越えた数。
VAP	TS クライアントに関係する仮想アクセスポイント
MAC Address	仮想アクセスポイントの MAC アドレス
SSID	TS クライアントの SSID
Statistics	
Network	クライアントに使用される無線インタフェース
Station	クライアントステーションの MAC アドレス
TS Identifier	TSPEC で設定されたトラフィックストリーム識別数（TID）。 範囲は 0–7 です。
TS Type	アクティブな TS を保持するクライアントのエントリ。アクティブなトラフィックストリームがない場合は、エントリもありません。
Access Category	トラフィックストリームのアクセスカテゴリです。(音声 / 映像)

項目	説明
Direction	トラフィックストリームの方向性です。以下の 3 つがあります。 • uplink（アップリンク） • downlink（ダウンリンク） • bidirectional（双方向）
From Station	無線クライアントから受信したパケットの数と量と、受信後に破棄されたパケットの量。以下のパケットについても表示されます。 • 超過 TSPEC • AP に必要とされても構築されなかった TSPEC
To Station	無線クライアントから送信されたパケットの数と量と、送信後に破棄されたパケットの量。以下のパケットについても表示されます。 • 超過 TSPEC • AP に必要とされても構築されなかった TSPEC

リンクの保全性のモニタリング

本アクセスポイントでは、各接続クライアントに対してその接続を検証するためにリンクの保全性のモニタリング機能を提供します。これを使用すると、アクセスポイントは、トラフィックが通過しない場合に数秒ごとにクライアントにデータパケットを送信します。これにより、通常のトラフィックの交換期間内であってもクライアントが範囲外に出てしまったことを検出することができます。データパケットが認識されないと、接続解除メッセージを受信しなくてもクライアントの接続は 300（秒）以内にリストから破棄されます。

Rogue AP Detection（不正アクセスポイントの検出）

Web マネージャ画面で参照しているアクセスポイント範囲にあるすべてのアクセスポイントのリアルタイム統計情報を提供します。「AP Detection」が有効な場合、無線は操作チャンネルから同帯域内の他のチャンネルのスキャンをします。「Refresh」ボタンをクリックして、画面を更新し、最新の情報を表示します。

「Rogue AP Detection」ページには次の二つのリストが存在します。:

- 「Detected Rogue AP List」— 帯域内にある既知の AP として認識されていない AP のリストです。
- 「Known AP List」— 帯域内にある既知の AP として認識されている AP のリストです。「Detected Rogue AP」リスト内で「Grant/ 許可」された AP、またはインポートされた AP リストの AP が表示されます。

無線ネットワークにある他のアクセスポイントの情報を参照します。

Status > Rogue AP Detection の順にメニューをクリックし、以下の画面を表示します。

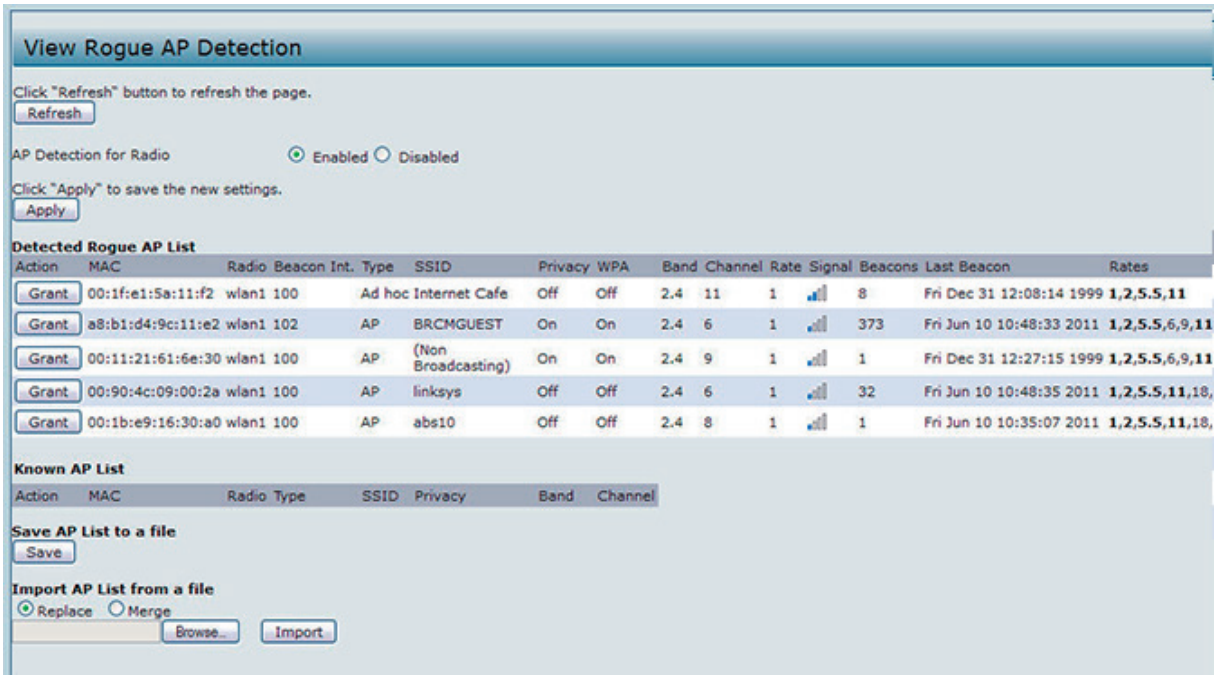


図 4-10　Rogue AP Detection 不正アクセスポイントの検出 画面

範囲内のアクセスポイントに関する情報を収集するためには、アクセスポイントにおける AP 検出を有効にする必要があります。

以下の表では隣接しているアクセスポイントに提供される情報について説明します。

項目	説明
AP Detection for Radio	• Enabled - Neighbor AP 検出を有効にして、帯域内の Neighbor AP に関する情報を収集します。 • Disabled - Neighbor AP 検出を無効にします。
Detected Rogue AP List（検出済み AP リスト）	
Action	「Grant」をクリックして検出された不正 AP リストから、既知の AP リストへ AP を移動させることが可能です。 「Detected Rouge AP List（検出された不正 AP リスト）」と「Known AP List」（既知の AP リスト）はあくまでも情報を表示するのみです。その他 DWL - x600AP はリスト内の検出済み AP に対して、セキュリティポリシーの変更などの管理動作を行うことはできません。
MAC	Neighbor AP の MAC アドレスを表示します。
Radio	どの無線インタフェースが Neighbor AP を検出したかを示します。 • wlan0（無線インタフェース 1） • wlan1（無線インタフェース 2）
Beacon Int.	この AP によって使用されるビーコン間隔を示します。 ビーコンフレームは無線ネットワークの存在を通知するために、アクセスポイントから定期的に送信されます。初期値では、ビーコンフレームは 100 ミリ秒に 1 度（1 秒に 10 回）送信されます。 ビーコン間隔は「Radio」タブで設定されます。（「Radio（無線の詳細設定）」（59 ページ）を参照してください。）
Type	デバイスのタイプを示します。 • AP - 隣接するデバイスが、Infrastructure モードで IEEE 802.11Wireless Networking Framework をサポートするアクセスポイントであることを示します。 • Ad hoc - アドホックモードで動作する隣接ステーションを示します。通常のアクセスポイントを使用せずに、アドホックモードに設定されたステーション同士が直接相互に通信します。アドホックモードは、ピアツーピアモードまたは Independent Basic Service Set（IBSS）として参照される IEEE 802.11 Wireless Networking Framework です。
SSID	アクセスポイントの識別子を示します。 SSID は、無線ローカルエリアネットワークを特定する 32 文字以内の半角英数字の文字列です。また、ネットワーク名としても参照されます。 SSID は「VAP」タブで設定されます。（「Load Balancing（ロードバランシングの設定）」（80 ページ）を参照してください。）
Privacy	隣接するデバイスにセキュリティ設定があるか否かを示します。 • Off - 隣接デバイスにおけるセキュリティモードが「None」（セキュリティなし）に設定されていることを示します。 • On - 隣接デバイスが適所に何らかのセキュリティを持っていることを示しています。 セキュリティは「VAP」画面でアクセスポイントに設定されます。
WPA	WPA セキュリティがアクセスポイントで「On」（有効）または「Off」（無効）であることを示します。
Band	アクセスポイントで使用している 802.11 のモードを示します。（例 IEEE 802.11a、IEEE 802.11b、および IEEE 802.11g モード） 表示された数値は、以下のマップに従ったモードを示します。 • 2.4 - IEEE 802.11b、802.11g、または 802.11n モード（または、モードの組み合わせ）を示します。 • 5 - IEEE 802.11a または 802.11n（または両モード）を示します。
Channel	アクセスポイントが現在ブロードキャストを行っているチャンネルを示します。 チャンネルとは、無線インタフェースがデータの送受信に使用する無線スペクトラムのある一部分を定義するものです。 チャンネルは **Manage > Radio** メニューで設定します。（「Radio（無線の詳細設定）」（59 ページ）を参照してください。）
Rate	アクセスポイントの現在の送信速度を示します。 現在の送信速度は常に「Supported Rates」に示される速度の 1 つになります。
Signal	このアクセスポイントが出力する信号強度が表示されます。バーの上でマウスポインタを動作させると、数値が表示されて強度（dB）で示します。
Beacons	最初に検出された後にアクセスポイントが受信したビーコンの総数を表示します。
Last Beacon	このアクセスポイントが最後のビーコンを受信した日時を表示します。
Rates	隣接しているアクセスポイントのサポート速度、およびベーシック（通知される）速度を表示します。速度は Mbit/ 秒で示されます。 すべてのサポート速度が太い文字でベーシック速度と共に表示されます。 速度セットは **Manage > Radio** メニューの「Rate Sets」で設定します。（「Radio（無線の詳細設定）」（59 ページ）を参照してください。）
Known AP List（既知の AP リスト）	
Action	「Grant」をクリックして検出された不正 AP リストから、既知の AP リストへ AP を移動させることが可能です。 「Detected Rouge AP List（検出された不正 AP リスト）」と「Known AP List」（既知の AP リスト）はあくまでも情報を表示するのみです。その他 DWL - x600AP はリスト内の検出済み AP に対して、セキュリティポリシーの変更などの管理動作を行うことはできません。
MAC	Neighbor AP の MAC アドレスを表示します。

項目	説明
Radio	どの無線インタフェースが Neighbor AP を検出したかを示します。 • wlan0（無線インタフェース 1） • wlan1（無線インタフェース 2）
Type	デバイスのタイプを示します。 • AP - 隣接するデバイスが、Infrastructure モードで IEEE 802.11Wireless Networking Framework をサポートするアクセスポイントであることを示します。 • Ad hoc - アドホックモードで動作する隣接ステーションを示します。通常のアクセスポイントを使用せずに、アドホックモードに設定されたステーション同士が直接相互に通信します。アドホックモードは、ピアツーピアモードまたは Independent Basic Service Set（IBSS）として参照される IEEE 802.11 Wireless Networking Framework です。
SSID	アクセスポイントの識別子を示します。 SSID は、無線ローカルエリアネットワークを特定する 32 文字以内の半角英数字の文字列です。また、ネットワーク名としても参照されます。 SSID は「VAP」タブで設定されます。（「Load Balancing（ロードバランシングの設定）」（80 ページ）を参照してください。）
Privacy	隣接するデバイスにセキュリティ設定があるか否かを示します。 • Off - 隣接デバイスにおけるセキュリティモードが「None」（セキュリティなし）に設定されていることを示します。 • On - 隣接デバイスが適所に何らかのセキュリティを持っていることを示しています。 セキュリティは「VAP」画面でアクセスポイントに設定されます。
Band	アクセスポイントで使用している 802.11 のモードを示します。（例 IEEE 802.11a、IEEE 802.11b、および IEEE 802.11g モード） 表示された数値は、以下のマップに従ったモードを示します。 • 2.4 - IEEE 802.11b、802.11g、または 802.11n モード（または、モードの組み合わせ）を示します。 • 5 - IEEE 802.11a または 802.11n（または両モード）を示します。
Channel	アクセスポイントが現在ブロードキャストを行っているチャンネルを示します。 チャンネルとは、無線インタフェースがデータの送受信に使用する無線スペクトラムのある一部分を定義するものです。 チャンネルは **Manage > Radio** メニューで設定します。（「Radio（無線の詳細設定）」（59 ページ）を参照してください。）

Saving and Importing the Known AP List（既知 AP リストのインポートと保存）

既知の AP リストをファイルに保存するには、追加された全ての AP の MAC アドレスが既知 AP リストに存在している必要があります。初期値ではファイル名は「Rogue1.cfg」になります。テキストエディタか WEB ブラウザを使ってファイルを参照することが可能です。

保存した既知の AP のリストをインポートするには、他の DWL-x600AP シリーズからか、またはテキストファイルとして作成されたリストを使用します。リストに AP の MAC アドレスが記載されている場合、「Rogue/ 不正」AP として識別されることはありません。

ファイルから AP リストをインポートするには以下の手順を行います。:

1. 既存のリストに新しい既知 AP リストを置き換えるか、インポートするファイルから既知 AP リストを追加するか選択します。

- 「Replace」オプションをクリックするとインポートする新しい既知 AP リストに置き換えられます。
- 「Merge」オプションをクリックすると既存の AP リストにインポートする AP リストを追加します。

2. 「Browse」をクリックして、インポートするファイルを選択します。

インポートするファイル拡張子が「.txt」または「.cfg」である必要があります。ファイル内の MAC アドレスは 16 進数形式で各オクテットがコロンで分割されたフォーマットである必要があります。（例）「00:11:22:33:44:55」各エントリはスペースで別れている必要があります。既知の AP としてリストに記載されるには MAC アドレスは必須です。

3. 「Import」をクリックします。
インポートが終了すると画面が更新され、既知 AP リストに新しく追加された AP の MAC アドレスが表示されます。

Managed AP DHCP（管理アクセスポイントの DHCP 情報の表示）

本アクセスポイントは、最初の DHCP 要求に対する DHCP 応答を通じてネットワーク上の D-Link 統合スイッチについて学習します。ここでは、アクセスポイントがご使用のネットワーク上の DHCP サーバから学習した最大 4 つの D-Link 統合スイッチの DNS 名または IP アドレスを表示します。

スイッチの IP アドレス情報を持つアクセスポイントの DHCP 要求に応じるように DHCP サーバを設定する方法については、スイッチの操作マニュアルを参照してください。

Status > Managed AP DHCP の順にメニューをクリックし、以下の画面を表示します。

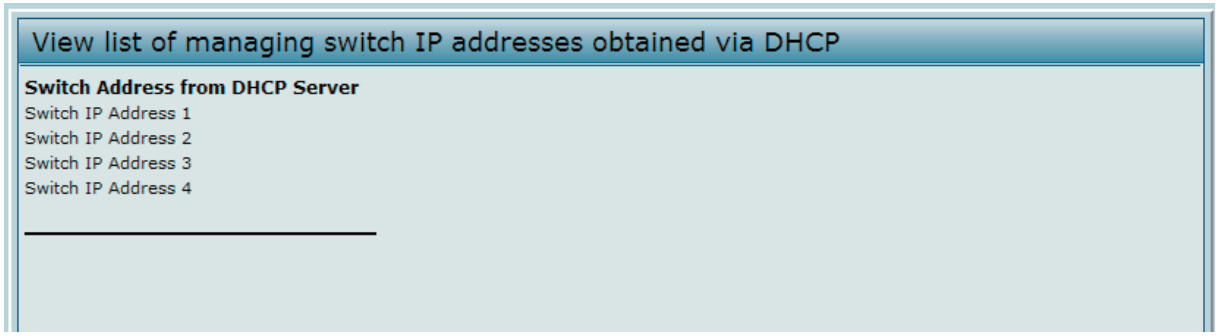

View list of managing switch IP addresses obtained via DHCP
Switch Address from DHCP Server
Switch IP Address 1
Switch IP Address 2
Switch IP Address 3
Switch IP Address 4

図 4-11　DHCP 経由で取得した管理スイッチの IP アドレスリストの参照 画面

TSPEC Status and Statistics（TSPEC ステータスと統計情報の参照）

「TSPEC Status and Statistics」ページでは、

- 無線による TSPEC セッションの要約情報
- VAP による TSPEC セッションの要約情報
- 全ての無線インタフェースの TSPEC VAP のリアルタイム送受信統計情報

について表示します。

全ての送受信統計情報は AP が起動してからの総計となります。AP を再起動した場合、再起動してからの統計情報となります。
「TSPEC Status and Statistics」タブをクリックして以下の画面を表示します。

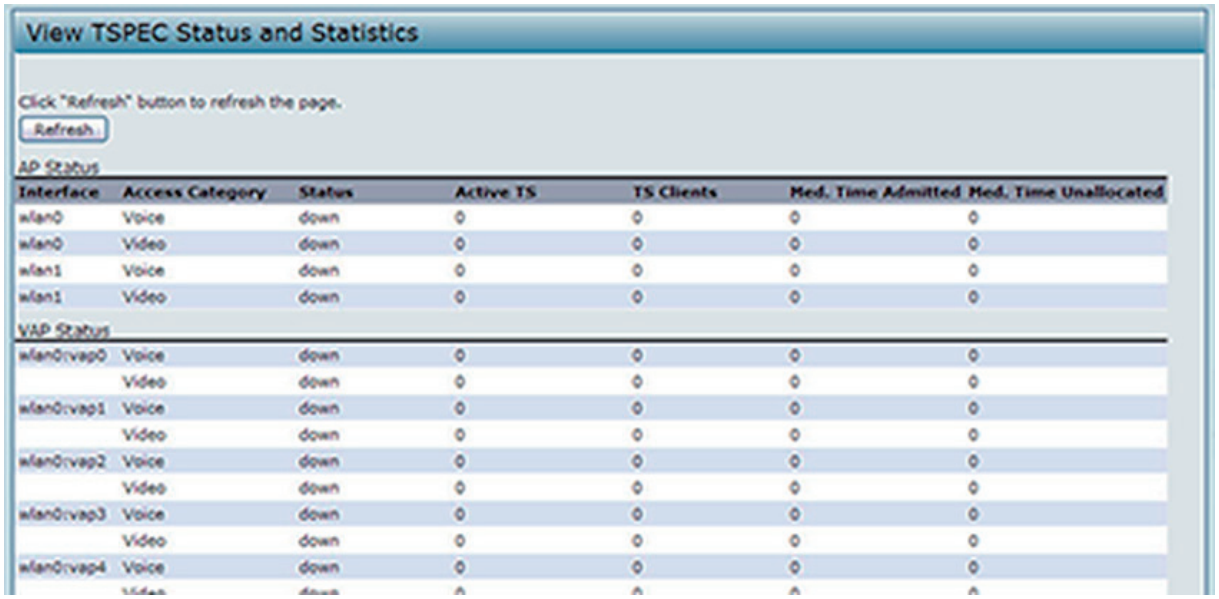

View TSPEC Status and Statistics
Click "Refresh" button to refresh the page.
Refresh
AP Status
Interface Access Category Status Active TS TS Clients Med. Time Admitted Med. Time Unallocated
wlan0 Voice down 0 0 0 0
wlan0 Video down 0 0 0 0
wlan1 Voice down 0 0 0 0
wlan1 Video down 0 0 0 0
VAP Status
wlan0vap0 Voice down 0 0 0 0
Video down 0 0 0 0
wlan0vap1 Voice down 0 0 0 0
Video down 0 0 0 0
wlan0vap2 Voice down 0 0 0 0
Video down 0 0 0 0
wlan0vap3 Voice down 0 0 0 0
Video down 0 0 0 0
wlan0vap4 Voice down 0 0 0 0

図 4-12　TSPEC Status and Statistics 画面

以下の表は、画面の各項目を説明します。

項目	説明
AP and VAP Status	
Interface	「Radio」または「VAP」インタフェースのどちらかを表示します。
Access Category	トラフィックストリームの種類（音声 / 映像）を示す現在のアクセスカテゴリを表示します。
Status	関連するアクセスカテゴリの TSPEC セッションが有効または無効を表示します。 （設定上のステータスを表示しており、現在の動作状況を表示しているとは限りません。）

項目	説明
Active TS	無線とアクセスカテゴリで現在動作中の TSPEC トラフィックストリームの数を表示します。
TS Clients	無線とアクセスカテゴリで現在動作中の TSPEC トラフィックストリームクライアントの数を表示します。
Medium Time Admitted	本アクセスカテゴリでデータ送信を行う「medium」(帯域) に配分された時間。「32 μsec/sec」単位で計算されます。本値はこのトラフィックストリームに許可された帯域の最大帯域以下である必要があります。
Medium Time Unallocated	本アクセスカテゴリで使用されていない「medium」(帯域) に配分された時間。「32 μsec/sec」単位で計算されます。
Transmit and Receive Statistics	
Total Packets	指定のアクセスカテゴリの無線で受信 / 送信された TS パケットの総量。
Total Bytes	指定のアクセスカテゴリの無線で受信 / 送信された TS バイトの総量。
Total Voice Packets	指定の VAP の無線で受信 / 送信された TS 音声パケットの総量。
Total Voice Bytes Total	指定の VAP の無線で受信 / 送信された TS 音声バイトの総量。
Video Packets Total	指定の VAP の無線で受信 / 送信された TS 映像パケットの総量。
Video Bytes	指定の VAP の無線で受信 / 送信された TS 映像バイトの総量。

TSPEC AP Statistics（TSPEC AP 統計情報の参照）

「TSPEC AP Statistics」TSPEC AP 統計情報のページでは AP によって許可 / 破棄された音声 / 映像トラフィックストリームの情報について表示します。
「TSPEC AP Statistics」タブをクリックします。

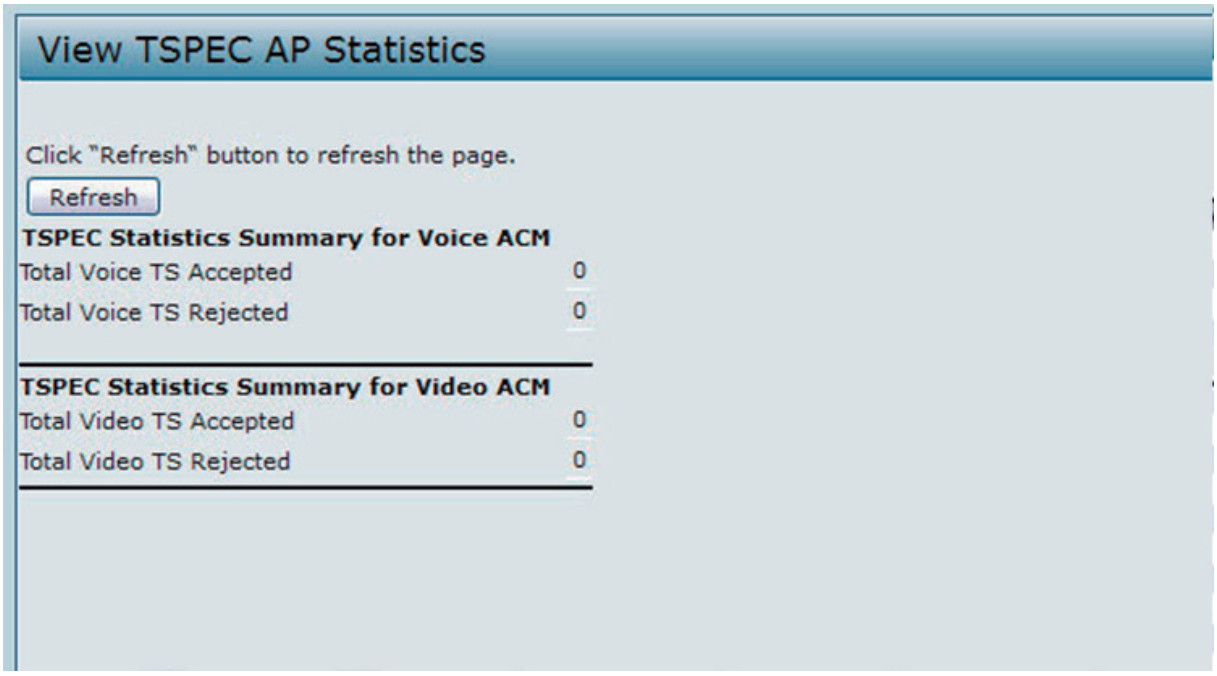

View TSPEC AP Statistics
Click "Refresh" button to refresh the page.
Refresh
TSPEC Statistics Summary for Voice ACM
Total Voice TS Accepted 0
Total Voice TS Rejected 0
TSPEC Statistics Summary for Video ACM
Total Video TS Accepted 0
Total Video TS Rejected 0

図 4-13　TSPEC AP Statistics 画面

以下の表は、画面の各項目を説明します。

項目	説明
TSPEC Statistics Summary for Voice ACM	許可された、または破棄された音声トラフィックストリームの総量。
TSPEC Statistics Summary for Video ACM	許可された、または破棄された映像トラフィックストリームの総量。

Radio Statistics（無線統計情報の参照）

「Radio Statistics」ページでは本アクセスポイントで送受信されたパケット / バイトについての詳しい情報を表示します。

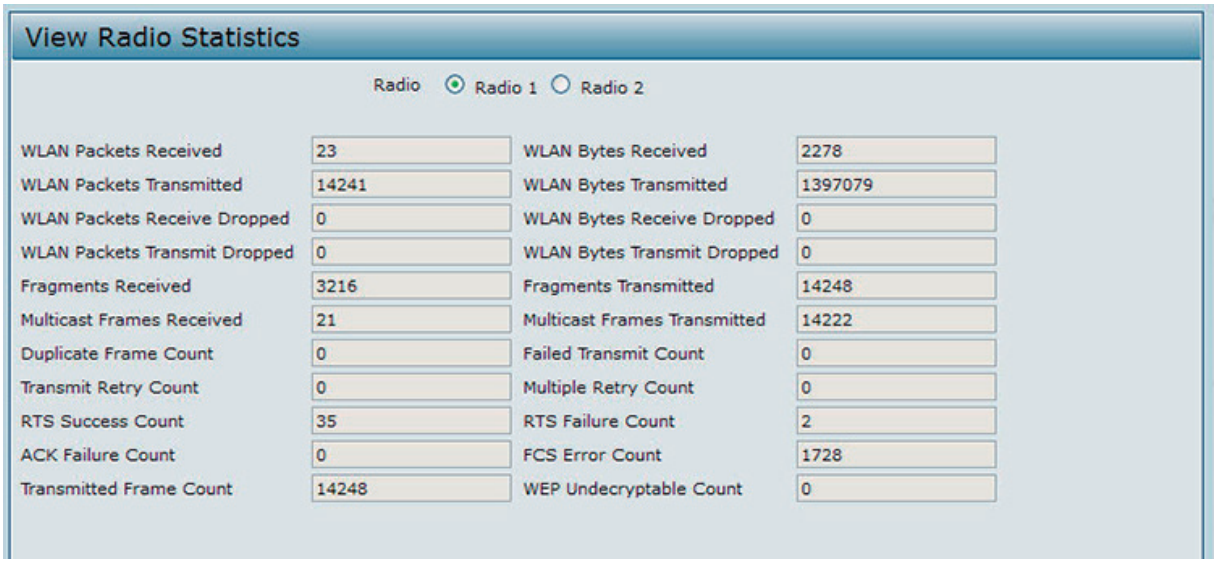


図 4-14　Radio Statistics 画面

以下の表は、画面の各項目を説明します。

項目	説明
Radio	「1」または「2」を選択して、参照する無線帯域を指定します。
WLAN Packets Received	無線インタフェース上でアクセスポイントが受信した総パケット数。
WLAN Bytes Received	無線インタフェース上でアクセスポイントが受信した総データ量。単位はバイトです。
WLAN Packets Transmitted	無線インタフェース上でアクセスポイントが送信した総パケット数。
WLAN Bytes Transmitted	無線インタフェース上でアクセスポイントが送信した総データ量。単位はバイトです。
WLAN Packets Receive Dropped	無線インタフェース上でアクセスポイントが受信し、破棄されたパケット数。
WLAN Bytes Receive Dropped	無線インタフェース上でアクセスポイントが受信し、破棄されたデータ量（バイト）。
WLAN Packets Transmit Dropped	無線インタフェース上でアクセスポイントが送信し、破棄されたパケット数。
WLAN Bytes Transmit Dropped	無線インタフェース上でアクセスポイントが送信し、破棄されたデータ量（バイト）。
Fragments Received	正しく受信したタイプがデータまたは管理の MPDU フレーム数。
Fragments Transmitted	送信したタイプがデータまたは管理で、個別アドレスまたはマルチキャストアドレスを含む MPDU フレーム数。
Multicast Frames Received	受信した宛先 MAC アドレス中にマルチキャストビットが設定されている MSDU フレーム数。
Multicast Frames Transmitted	正しく送信した宛先 MAC アドレス中にマルチキャストビットが設定されている MSDU 数。
Duplicate Frame Count	シーケンス制御フィールドで duplicate（冗長）と示されているフレームを受信した回数。
Failed Transmit Count	Short retry limit/Long retry limit 超過により、MSDU が正しく送信されなかった回数。
Transmit Retry Count	1 度以上のリトライ後に MSDU が正しく送信された回数。
Multiple Retry Count	2 度以上のリトライ後に MSDU が正しく送信された回数。
RTS Success Count	RTS フレームの応答として受信された CTS フレームの数。
RTS Failure Count	RTS フレームの応答として受信されなかった CTS フレームの数。
ACK Failure Count	想定していた ACK フレームが受信されなった数。
FCS Error Count	受信した MPDU により検知した FCS エラー数。
Frames Transmitted	送信に成功した MSDU の数。
WEP Undecryptable Count	暗号化されたフレームのうち、暗号化の必要なしと示されているもの、または受信デバイスがプライバシーオプションを使用していないために廃棄されたフレームの数。

Email Alert Status（E メールアラートステータスの参照）

「Email Alert Operational Status」はアクセスポイントで起動しているシスログメッセージを基本にした E メールアラートです。
「Email Alert Operational 」ステータスは「**Status > Email Alert Status** 」から以下を表示します、

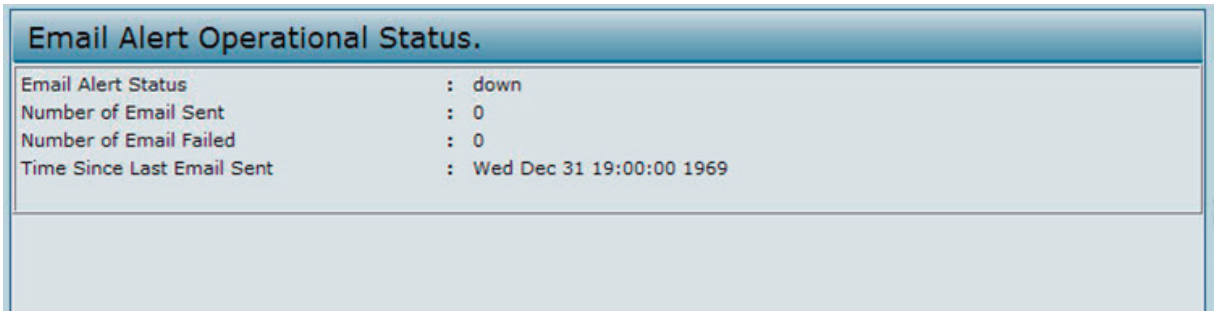

Email Alert Operational Status.
Email Alert Status : down
Number of Email Sent : 0
Number of Email Failed : 0
Time Since Last Email Sent : Wed Dec 31 19:00:00 1969

図 4-15　Email Alert Status 画面

以下の表は、画面の各項目を説明します。

項目	説明
Email Alert Status	E メールアラートのステータスです。「Up/Down」から確認します。. 初期値「Down」です。
Number of Email Sent	送信した E-Mail の総量です。初期値は 0 です。
Number of Email Failed	送信に失敗した E-Mail の総量です。初期値は 0 です。
Time Since Last Email Sent	最後の E-mail が送られてきてからの時間です。

第 5 章　Manage（アクセスポイントの管理）

本製品の管理方法について説明します。以下のサブセクションがあります。

設定項目	説明	参照ページ
Ethernet Settings（イーサネット設定）	本製品の LAN インタフェースを設定します。	55 ページ
Wireless Settings（無線設定）	本製品の無線インタフェースに基本的な設定します。	57 ページ
Radio（無線の詳細設定）	本製品の無線インタフェースに詳細な設定を行います。	59 ページ
Scheduler Configuration（スケジューラの設定）	消費電力の削減や無線スケジュールを業務時間のみの稼動に制限してセキュリティ強化するなどために使用します。	63 ページ
Scheduler Association Settings（スケジューラ関連設定）	スケジューラプロファイルを有効にするために、無線または VAP と連携します。	65 ページ
VAP（仮想アクセスポイントの設定）	仮想アクセスポイントの設定を行います。	66 ページ
WDS（WDS の設定）	WDS の設定を行います。	74 ページ
MAC Authentication（MAC 認証によるアクセス制御）	無線クライアントの MAC アドレスに基づいてアクセスポイント経由でネットワークへのアクセスを制御します。	78 ページ
Load Balancing（ロードバランシングの設定）	ロードバランシングの設定を行います。	80 ページ
Managed Access Point（管理アクセスポイントの設定）	管理アクセスポイントの設定を行います。	81 ページ
Authentication（802.1X 認証の設定）	802.1X サプリカントのユーザ名とパスワードを設定します。	83 ページ
Management ACL（管理アクセスコントロールリストの作成）	アクセスコントロールリスト（ACL）を作成します。	84 ページ

本セクションの機能に対する設定画面は、メインメニューの「Manage」にあります。

Ethernet Settings（イーサネット設定）

DHCP と VLAN 情報を含む有線インタフェースの初期設定は、すべてのネットワークをサポートしていません。

初期値では、本製品上の DHCP クライアントは自動的にネットワーク情報に関する要求をブロードキャストします。スタティック IP アドレスを使用する場合、DHCP クライアントを無効にして、手動で IP アドレスおよび他のネットワーク情報を設定する必要があります。

管理用 VLAN は初期値で VLAN 1 のタグなし VLAN です。ネットワーク上に異なる VLAN ID を使用した管理用 VLAN が存在している場合は、アクセスポイントの管理用 VLAN の VLAN ID を変更する必要があります。

LAN 設定を行うためには、**Manage > Ethernet Settings** の順にメニューをクリックし、以下の画面を表示します。

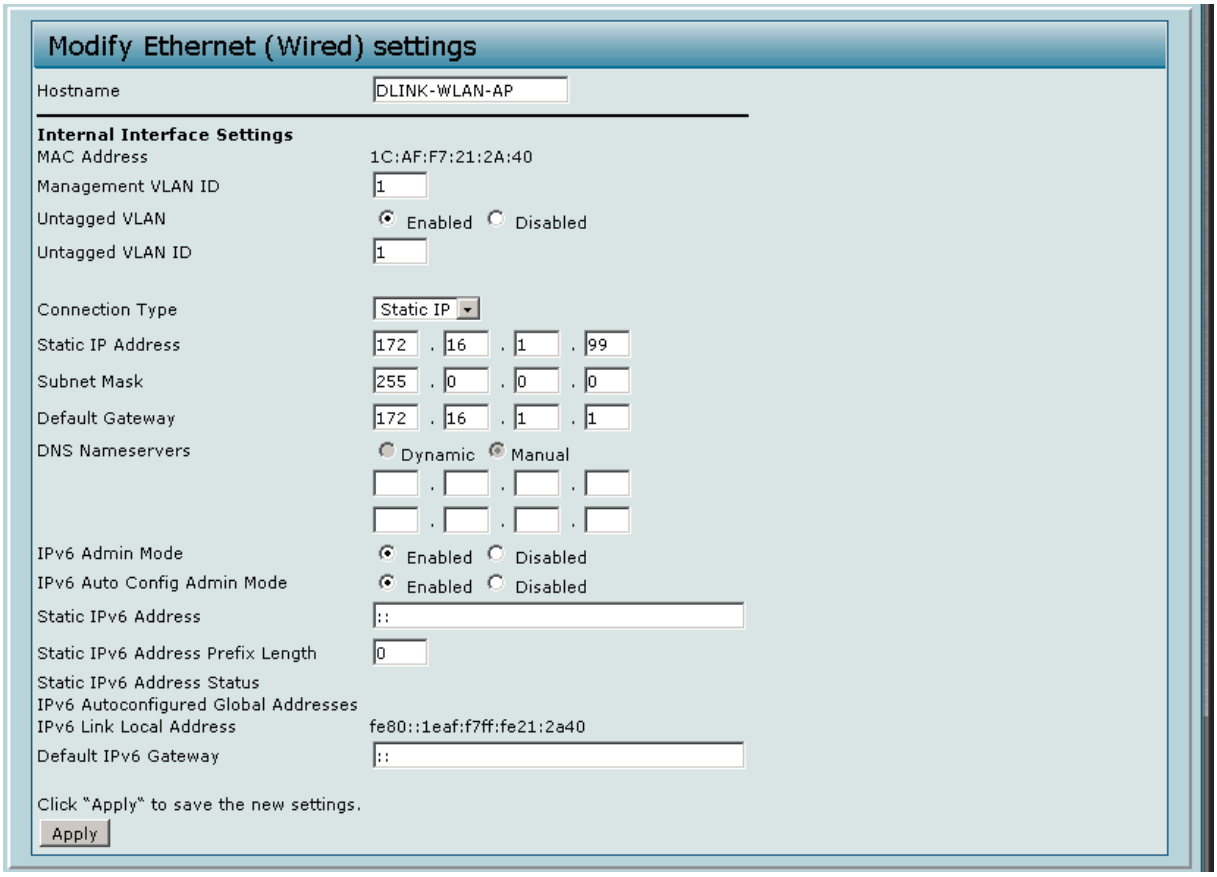


図 5-1　イーサネット（有線）設定の編集 画面

参照および設定する項目を示します。

項目	説明
Host Name	テキストボックスにアクセスポイントの DNS 名（ホスト名）を入力します。 DNS 名は、以下の条件を満たす必要があります。 • 1-63 半角英字 • 英数字、および「-」（ダッシュ）のみ指定します。 • 英字で開始し、英字または数字で終了する必要があります。
MAC Address	このアクセスポイントにおけるイーサネットポートの LAN インタフェースの MAC アドレスを表示します。これは参照用欄で、変更することはできません。
Management VLAN ID	管理 VLAN はアクセスポイントにアクセスするのに使用する IP アドレスに関連付けされている VLAN です。管理 VLAN ID の初期値は 1 です。 管理 VLAN 用に 1 から 4094 までの番号を提供します。
Untagged VLAN	無効にすると、すべてのトラフィックは VLAN ID をタグ付けされます。 初期値では、本アクセスポイントのすべてのトラフィックは VLAN 1 を使用し、タグなしになっています。つまり、Untagged VLAN を無効にするか、タグなしトラフィックの VLAN ID を変更するか、または RADIUS を使用して VAP かクライアントの VLAN ID を変更するまで、すべてのトラフィックはタグなしとなります。
Untagged VLAN ID	タグなし VLAN ID に 1 から 4094 までの番号を提供します。本欄に指定する VLAN 上のトラフィックは、VLAN ID をタグ付けされません。
Connection Type	• DHCP - UAP は DHCP サーバから IP アドレス、サブネットマスク、DNS、およびゲートウェイ情報を取得します。 • Static IP -「Static IP Address」、「Subnet Mask」、および「Default Gateway」欄に情報を入力する必要があります。
Static IP Address	スタティック IP アドレスを入力します。本欄は、「Connection Type」に「DHCP」を選択すると無効になります。

項目	説明
Subnet Mask	サブネットマスクを入力します。
Default Gateway	デフォルトゲートウェイを入力します。
DNS Nameservers	DNS のモードを選択します。 • Dynamic - DNS サーバの IP アドレスは DHCP を通じて自動的に割り当てられます。「Connection Type」に「DHCP」を指定した場合にだけ、このオプションは利用可能です。 • Manual - メイン名を解決するためにスタティック IP アドレスを割り当てる必要があります。
IPv6 Admin Mode	アクセスポイントへの IPv6 管理アクセスを有効、または無効にします。
IPv6 Auto Config Admin Mode	アクセスポイントへの IPv6 自動アドレス設定を有効、または無効にします。 「IPv6 Auto Config Admin Mode」が有効な場合、自動 IPv6 アドレス設定とゲートウェイ設定は、LAN ポートで受信した Router Advertisements を処理することで許可されます。アクセスポイントは、複数の自動設定された IPv6 アドレスを持つことができます。
Static IPv6 Address	スタティックな IPv6 アドレスを入力します。アドレスが既に自動的に設定されていても、アクセスポイントはスタティックな IPv6 アドレスを持つことができます。
Static IPv6 Address Prefix Length	スタティック IPv6 のプレフィックス長を 0-128 の範囲で入力します。
IPv6 Autoconfigured Global Addresses	自動的に 1 つ以上の IPv6 アドレスをアクセスポイントに割り当てている場合に、アドレスが表示されます。
IPv6 Link Local Address	IPv6 Link Local アドレスを表示します。これは、ローカルな物理リンクによって使用される IPv6 アドレスです。これは、IPv6 Neighbor Discovery プロセスを使用することで割り当てられるため、リンクローカルアドレスを設定するはできません。
Default IPv6 Gateway	デフォルト IPv6 ゲートウェイを入力します。

注意 設定を実施後に「Apply」ボタンをクリックして変更を適用して設定を保存します。設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

Wireless Settings（無線設定）

無線設定では、特にアクセスポイント（802.11 モードとチャンネル）内の無線デバイスに接続する LAN インタフェース、およびアクセスポイント（アクセスポイントの MAC アドレス）に対するネットワークインタフェースに接続する LAN インタフェースについて説明します。

無線インタフェースを設定します。

Manage > Wireless Settings の順にメニューをクリックし、以下の画面を表示します。

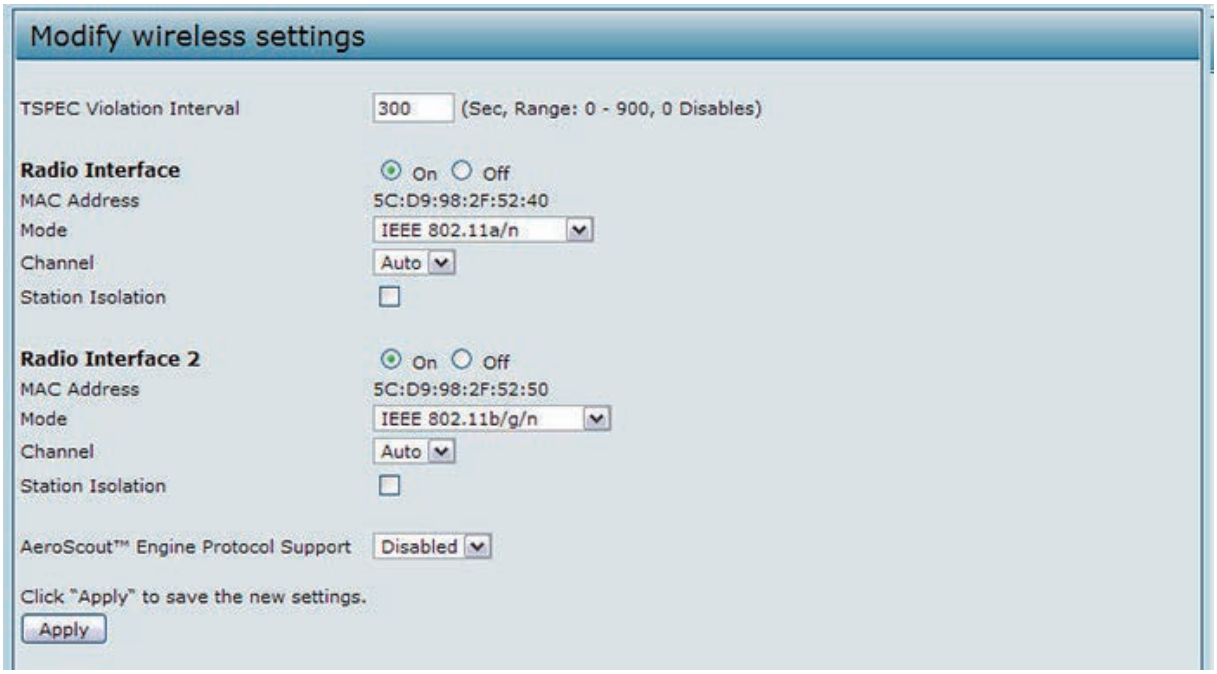


図 5-2　無線設定の編集 画面

注意　無線インタフェース設定は、無線インタフェース 1 と無線インタフェース 2 の両方に適用されます。

利用可能な項目と設定オプションについて説明します。

項目	説明
TSPEC Violation Interval	クライアントが権限手順を遵守していない場合にレポート（システムログと SNMP とラップ）を送信するまでのインターバル（秒）を指定します。
Radio Interface / Radio Interface2	「On」または「Off」ラジオボタンを選択して、無線インタフェースをオンまたはオフにします。
MAC Address	無線インタフェース 1 と 2 の MAC アドレスを表示します。 MAC アドレスは、どんなデバイスにも永久的で、固有なハードウェアアドレスであり、ネットワークに対するインタフェースを表します。MAC アドレスはメーカによって割り当てられるもので、変更することはできません。インタフェースの固有な識別子として情報の目的のためにここで示します。
Mode	各無線インタフェースに対して以下のモードから一つ選択します。 • Radio Interface - IEEE 802.11a - 802.11a クライアントだけがアクセスポイントに接続できます。 - IEEE 802.11a/n - 802.11a および 802.11n クライアントが 5GHz 帯でアクセスポイントに接続できます。 - 5 GHz IEEE 802.11n - 802.11n クライアントだけが 5GHz 帯でアクセスポイントに接続できます。 • Radio Interface2 - IEEE 802.11b/g - 802.11b および 802.11g クライアントがアクセスポイントに接続できます。 - IEEE 802.11b/g/n - 802.11b、802.11g および 802.11n クライアントが 2.4GHz 帯でアクセスポイントに接続できます。 - 2.4 GHz IEEE 802.11n - 802.11n クライアントだけが 2.4GHz 帯でアクセスポイントに接続できます。
Channel	チャンネルを選択します。 利用可能なチャンネルの範囲は、無線インタフェースのモードによって決定されます。チャンネル設定に「Auto」を選択すると、アクセスポイントは、利用可能なチャンネルをスキャンして、トラフィックが検出されないチャンネルを選択します。チャンネルとは、無線インタフェースがデータの送受信に使用する無線スペクトラムのある一部分を定義するものです。各モードは多くのチャンネルを提供しますが、スペクトルが米連邦通信委員会（FCC）または国際電気通信連合（ITU-R）などの国家や国家をまたがる機関によってどう認可されるかによって異なります。

項目	説明
Station Isolation	ステーションアイソレーションを有効にするためには、横にあるチェックボックスを選択します。 • 無効にした場合 - 無線クライアントは、通常通りアクセスポイントを経由してトラフィックを送信することで相互に通信できます。 • 有効にした場合 - アクセスポイントは同じ VAP にある無線クライアント間の通信をブロックします。アクセスポイントは、無線クライアント間だけでなくネットワークの無線クライアントと有線デバイス間のデータトラフィック、WDS リンクを経由するデータトラフィック、および異なる VAP に接続する他の無線クライアントとのデータトラフィックを許可します。
AeroScout ™ Engine Protocol Support	「AeroScout Engine」は無線ネットワークの位置情報提供サービスです。「AeroScout」プロトコルを有効にすると使用可能になります。 初期値では無効です。「有効」にすると「Aeroscout」対応機器が認識され分析のためデータが「Aeroscout Engine (AE)」に送信されます。「AE」は「STA」や「AP」そして「AeroScout」対応の 802.11 有効 RFID 機器やタグなどの位置情報を明らかにします。「AE」は AP によって検出された RF 機器についての情報を収集する AE プロトコルをサポートする機器と通信をします。AE プロトコルの使用については、D-Link は AE と AP の直接のやり取りをサポートします。管理モードで使用している時、「AE」は情報を収集した管理アクセスポイントの IP アドレスを設定します。 通常の無線スイッチでは AE 機器との通信はできません。 注意：「AeroScout」タグは「T2」「T3」ハードウェアのみサポートします。他のタグモデルは、対応している AeroScout プロトコルが「AeroScout Engine - Access Point Interface Specification, version 2.1」に準じている場合のみサポートしています。 注意：「AeroScout」タグは「802.11 b/g」モードでのみ使用できます。それにより Therefore, network administrators who use the 「AeroScout」タグを使用するネットワーク管理者は少なくとも 1 つは「802.11b/g」または「802.11b/g/n」モードで検出されるタグの AP の無線である必要があります。「2.4 GHz IEEE 802.11」モード、または「5GHZ」モードでは「AeroScout」タグは検出できません。 注意：「AE」プロトコルは不正と認識された AP も許可してしまいます。「D-Link」AP はこの機能をサポートせず、不正と選出された AP のレポートを行いません。

注意 無線設定を実施後に「Apply」ボタンをクリックして変更を適用し、設定を保存します。設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

802.11h 無線モードの使用

IEEE 802.11h 規格には、以下に示す重要項目があります。

- 802.11h は 802.11a インタフェースでのみ動作します。これは、802.11b または 802.11g には必要とされません。
- 802.11h が有効なドメインで操作を行う場合、アクセスポイントは割り当てたチャンネルの使用を試みます。チャンネルが前の電波検出でブロックされたか、またはアクセスポイントがチャンネル上に電波を検出すると、アクセスポイントは自動的に異なるチャンネルを選択します。
- 802.11h が有効にされると、アクセスポイントは、電波走査のために少なくとも 60 秒間、5GHz 帯域では操作されません。
- 802.11h が有効である場合、WDS リンクの設定は困難かもしれません。これは WDS リンクにおける 2 つのアクセスポイントの操作チャンネルがチャンネルの使用と電波干渉によっては変更を続ける可能性があるためです。両方のアクセスポイントが同じチャンネルで動作する場合にだけ、WDS は動作します。WDS に関する詳しい情報については、「Load Balancing（ロードバランシングの設定）」（80 ページ）を参照してください。

Enabling AeroScout ™ Engine Support（AeroScout ™ エンジンを有効にする）

「AeroScout Engine/ エアロスカウトエンジン」(AE) は「AeroScout 社」がプロデュースする位置情報サービスのソフトウェアです。「AE」は 802.11 対応の AeroScout 機器の物理的な位置を測定することが可能です。「AE」は AP によって検出された RF 機器についての情報を収集するための、AE 有効なプロトコルを保持する AP と連携します。
DWS-4000 スイッチは AE と AP の直接的なコミュニケーションをサポートします。管理モードでの操作時には AE は情報を収集する管理 AP の IP アドレスを設定します。DWS-4000 スイッチ自体は AE とは連携しません。「AeroScout」タグは「802.11b/g」モードの時のみ有効です。その結果、「AeroScout」タグを使用するネットワーク管理者は「802.11b/g」または「802.11b/g/n」モードでタグが検出される AP の、少なくとも 1 つの無線を設定する必要があります。「2.4 GHz IEEE 802.11n」モードまたは「5 GHz」モードのどれかで設定された無線は、「AeroScout」タグを検出できません。「AeroScout」サポートを有効にするには「Configuring the AP Profile Global Settings」を参照します。

注意 「AeroScout」の製品とプロトコルのサポートには次の注意が必要です。：

- D-Link では「AeroScout」製品は販売していません。「AeroScout」に連絡して、「AeroScout」の機器、ソフトウェア、開発情報についてご確認ください。
- 「AE」プロトコルは AE サーバとアクセスポイント間の認証や暗号をサポートしません。
- 「AE」プロトコルは複数の雑多なモードでの無線操作を必要とします。これは、AP の BSSID へ向かうパケットのみ処理するのとは違い、AP は無線により検出されたすべてのパケットを受信、処理することを意味します。そしてこれは AP のスループットに影響します。

Radio（無線の詳細設定）

無線設定はアクセスポイントにおける無線デバイスの働きと物理的な媒体との相互作用を直接制御します。つまり、アクセスポイントが放出する電磁波のタイプと放出方法を制御します。

無線の詳細な設定を行います。

Manage > Radio の順にメニューをクリックし、以下の画面を表示します。選択するモードによって異なる設定を表示します。

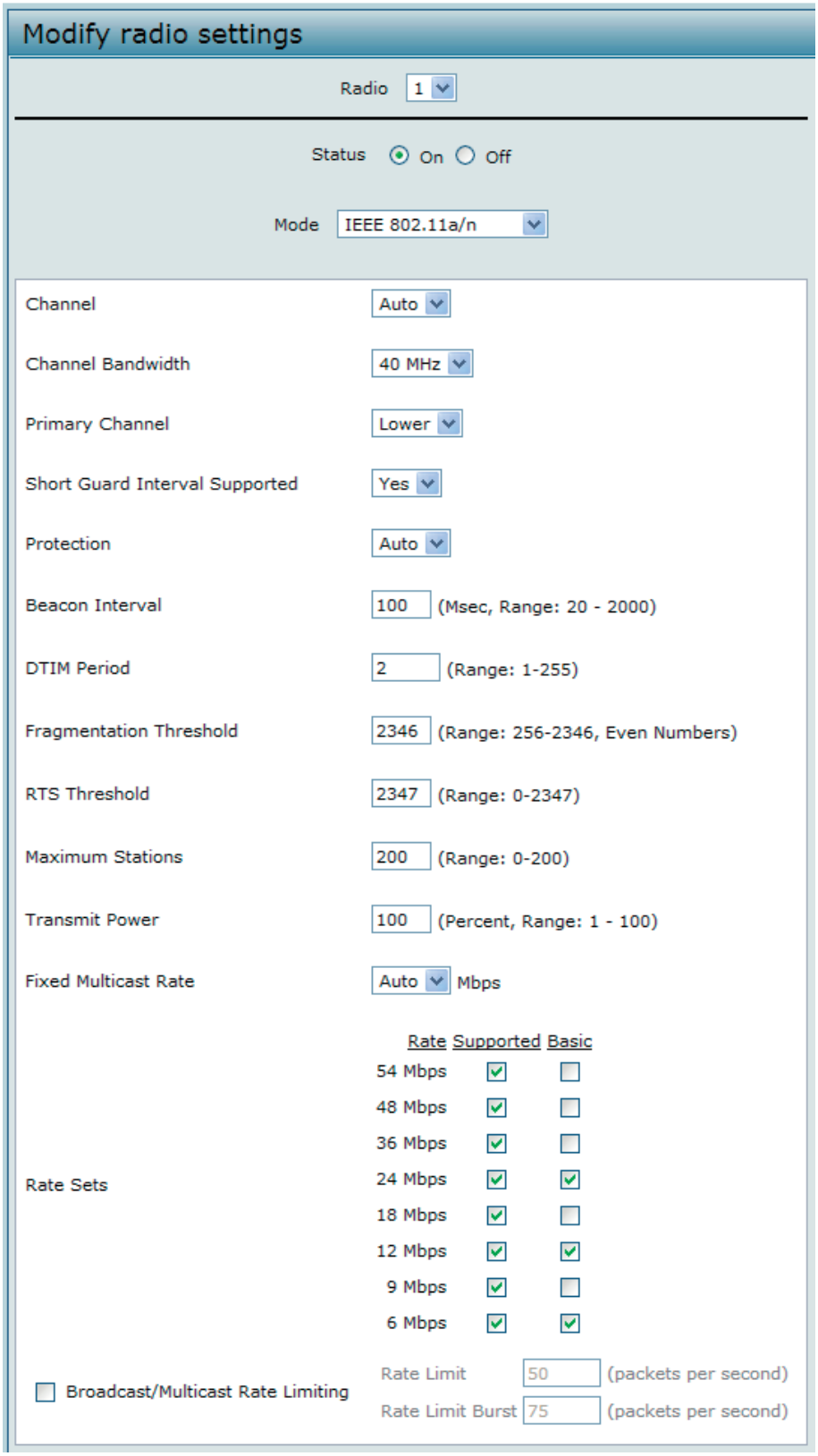


図 5-3　無線インタフェース設定の編集 画面

項目および設定オプションについて説明します。

項目	説明
Radio	「1」または「2」を選択して、設定する無線帯域を指定します。本画面の残りの設定はここで選択する無線帯域に適用されます。両方の無線帯域に設定を必ず行ってください。 Radio 1 は、5GHz 帯、Radio2 は 2.4GHz 帯で動作します。
Status	「On」または「Off」ラジオボタンを選択して、無線インタフェースをオンまたはオフにします。 無線インタフェースをオフにすると、アクセスポイントは配下のすべての無線クライアントに向けて接続解除フレームを送信します。この手順で無線インタフェースのシャットダウンが行われ、クライアントは他のアクセスポイントとの間で接続プロセスを開始します。
Mode	無線インタフェースが使用する物理層（PHY）の標準を定義します。 **注意** 利用可能なモードは国コード設定および選択した無線帯域に依存します。 各無線インタフェースに対して以下のモードから一つ選択します。 • Radio1 - IEEE 802.11a - IEEE 802.11a/n - 5 GHz IEEE 802.11n • Radio1 - IEEE 802.11b/g - IEEE 802.11b/g/n - 2.4 GHz IEEE 802.11n
Channel	チャンネルを選択します。 利用可能なチャンネルの範囲は、無線インタフェースのモードや国コード設定によって決定されます。チャンネル設定に「Auto」を選択すると、アクセスポイントは、利用可能なチャンネルをスキャンして、トラフィックが検出されないチャンネルを選択します。 チャンネルとは、無線インタフェースがデータの送受信に使用する無線スペクトラムのある一部分を定義するものです。各モードは多くのチャンネルを提供しますが、スペクトルが米連邦通信委員会（FCC）または国際電気通信連合（ITU-R）などの国家や国家をまたがる機関によってどう認可されるかによって異なります。
Channel Bandwidth （802.11a/n モードのみ）	802.11n 仕様では他のモードで利用可能な既存の 20MHz のチャンネルに加えて 40MHz 幅のチャンネルを容認しています。40MHz のチャンネルは、より高いデータ速度を可能にしますが、他の 2.4GHz および 5GHz デバイスが使用できるチャンネルが少なくなります。 チャンネル帯域幅の使用を 20MHz に制限するためには本欄を 20MHz のチャンネルに設定します。
Primary Channel （802.11a/n モードのみ）	チャンネル帯域幅を 40MHz に設定する場合にだけ、本設定を変更することができます。40MHz のチャンネルは、周波数領域で隣接している 2 個の 20MHz のチャンネルから構成されていると見なすことができます。 これらの 2 個の 20MHz のチャンネルはしばしば Primary と Secondary チャンネルと呼ばれます。Primary Channel は 20MHz のチャンネル帯域幅だけをサポートする 802.11n クライアントとレガシークライアントに使用されます。 以下のオプションの 1 つを選択します。 • Upper - 40MHz 帯域の上位 20MHz のチャンネルとして Primary Channel を設定します。 • Lower - 40MHz 帯域の下位 20MHz のチャンネルとして Primary Channel を設定します。
Short Guard Interval Supported	選択した無線モードに 802.11n が含まれる場合にだけ、本欄は利用可能です。 ガードインターバルは OFDM シンボル間のデッドタイム（ns）です。ガードインターバルは符号間干渉と搬送波間干渉（ISI、ICI）を防ぎます。802.11n モードでは、802.11a/g の定義する 800（ns）から 400（ns）にこのガードインターバルを短縮することが許容されています。 ガードインターバルの短縮によって、データ処理性能において 10% の改善をもたらすことができます。 以下のオプションの 1 つを選択します。 • Yes - アクセスポイントは、短いガードインターバルをサポートするクライアントと通信する場合に 400ns のガードインターバルを使用してデータを送信します。 • No - アクセスポイントは、800ns のガードインターバルを使用してデータを送信します。
STBC Mode	本項目は無線モードが 802.11n を選択した場合のみ表示されます。 「Space Time Block Coding」(STBC) はデータ送信の信頼性を高めるための、「802.11n」応用技術の一つです。データ送信は複数のアンテナを使用するため、少なくともデータストリームの 1 つにおいて受信システムはよりよい検出チャンスがあります。 「On」— AP は同時に複数のアンテナに同じデータストリームを送信します。 「Off」— AP は複数のアンテナで同じデータストリームを送信しません。

項目	説明
Protection	保護機能は、802.11 の伝送がレガシーステーションまたはアプリケーションで干渉を起こさないことを保証するルールを含んでいます。初期値では、これらの保護メカニズムは有効（Auto）です。保護が有効な場合、アクセスポイントの適用範囲内にレガシーデバイスがあると、保護メカニズムが呼び出されます。 これらの保護メカニズムを無効（Off）にすることができますが、保護をオフにすると、適用範囲内のレガシークライアントまたはアクセスポイントが 802.11n 伝送によって影響を受けることがあります。モードが 802.11b/g である場合にも、保護機能は利用可能です。保護がこのモードで有効とすると、802.11b クライアントとアクセスポイントを 802.11g の伝送から保護します。 **注意** この設定はアクセスポイントに接続するクライアントの能力に影響しません。
Beacon Interval	ビーコンフレームは無線ネットワークの存在を通知するために、アクセスポイントから定期的に送信されます。初期状態では、ビーコンフレームは 100（m 秒）に 1 度（1 秒に 10 回）送信されます。 20 - 2000 の範囲から値を指定します。
DTIM Period	1 - 255 のビーコンの DTIM 間隔を指定します。 DTIM メッセージはビーコンフレームに含まれる要素です。DTIM は省電力モード中の無線クライアント向けのデータがアクセスポイントに送信待ちとしてバッファされていることを示しています。 ここで指定する DTIM Period（DTIM 間隔）は、本アクセスポイントの配下にあるクライアントが、アクセスポイントにバッファされているデータを確認する間隔を示します。数字はビーコンの数で表します。 例えば、本欄に 1 を入力した場合、バッファされたデータの確認は、ビーコンフレーム送信ごとにアクセスポイントで行われます。10 を入力した場合は 10 回のビーコンフレーム送信に 1 度の確認となります。
Fragmentation Threshold	フレームサイズのしきい値を 256-2,346（バイト）で設定します。 フラグメントしきい値は、ネットワーク上で伝送されるパケットサイズを制限する方法です。パケットが設定したフラグメント化のしきい値を超えていると、フラグメント化機能はアクティブとなり、パケットは複数の 802.11 フレームとして送信されます。 送信パケットが、しきい値以下であると、フラグメント化は使用されません。 しきい値を最大値（2,346 バイト）に設定すると、フラグメント化は事実上無効になります。Aggregation が有効であると、フラグメント化は役割を全く果たしません。 フラグメント化は、必要とするフレームの分割と再構築の追加の作業のため、およびネットワークにおけるメッセージのトラフィックを増加させるためにより多くのオーバヘッドを伴います。 しかし、適切に設定されると、ネットワーク性能と信頼性を改善することができます。 （低いフラグメント化しきい値を使用することで）小さいフレームを送信すると、電子レンジとの干渉などいくつかの干渉問題に役に立つかもしれません。 初期値ではフラグメント化は無効です。電波干渉を疑わない場合にはフラグメント化を使用することをお勧めしません。各フラグメントに適用された追加ヘッダは、ネットワークでオーバヘッドを増加して、処理性能を大きく低下させます。
RTS Threshold	Request to Send（RTS）しきい値を 0-2347 の範囲で指定します。 RTS しきい値は、MPDU 内のオクテット数を示します。設定値より低いと RTS/CTS ハンドシェークは実行されません。この値を変更することで、特に多数のクライアントを抱えるアクセスポイントを通過するトラフィックフローを制御することができます。低い値を指定すると、RTS パケットは頻繁に送信されるようになります。これにより消費する帯域幅は増大し、パケットのスループットは低下します。一方、RTS パケットの送信数を増やす、混雑したネットワーク内で起こり得る干渉や衝突からの回避や、電磁波による干渉を軽減できるようになります。
Maximum Stations	本アクセスポイントに一度にアクセスできるステーションの最大数（0-200）を指定します。
Transmit Power	本アクセスポイントの送信電力レベルに対する割合（%）を入力します。 初期値は 100% ですが、これはアクセスポイントに最大のブロードキャスト範囲を与え、必要とされるアクセスポイント数を減らすことができるために、低い割合よりもコスト効果が高い場合があります。 ネットワーク性能を高めるためには、アクセスポイントをより近くに置いて、送信電力の値を減少させてください。これは、アクセスポイント間のオーバラップと干渉を抑制します。弱い無線信号はご使用のネットワークの物理的位置の外側には伝播しにくいため、低い送信電力設定がご使用のネットワークをより安全に保ちます。
Fixed Multicast Rate	アクセスポイントのマルチキャストトラフィック通信速度を選択します。
Legacy Rate Sets	アクセスポイントの通信速度設定、およびアクセスポイントが通知をする速度を指定します。 • Rates - Mbit/ 秒で表されます。 • Supported Rates Sets - アクセスポイントがサポートする通信速度です。複数の速度を選択することができます。チェックボックスをクリックすることで選択します。エラー率やアクセスポイントとクライアントとの距離などの要素を元に、アクセスポイントは最も効率の良い速度を自動的に選択します。 • Basic - ネットワーク内の他のアクセスポイントやクライアントとの通信を開始するために、アクセスポイントがネットワークに通知する通信速度です。一般的に、アクセスポイントがサポートする通信速度をブロードキャストするのが効率的です。

項目	説明
MCS (Data Rate)Settings（802.11a/n モードのみ）	本項目では無線にサポートされる「Modulation and Coding Scheme」(MCS) インデックス値を表示します。それぞれのインデックスは個別に有効 / 無効に設定できます。
Broadcast/Multicast Rate Limiting	マルチキャストとブロードキャスト速度制限を有効にすると、ネットワークを経由して送信されるパケット数を制限することによって、全体的なネットワーク性能を改善することができます。 初期値では、本オプションは無効です。これを有効にするまで、以下の項目は無効にされます。
Rate Limit	マルチキャストとブロードキャストトラフィックに設定する速度制限を入力します。制限値は 1 秒あたり 1 以上 50 未満のパケット数とすべきです。この速度制限を下回るトラフィックはいずれも、常に適合して適切な宛先に送信されます。初期値と最大速度制限値は 50 パケット / 秒です。
Rate Limit Burst	速度を制限するバースト値を設定すると、すべてのトラフィックが速度制限を超える前のトラフィックバーストの量を決定します。このバースト制限は、設定した速度制限を超えるネットワーク上のトラフィックの間欠バーストを容認します。初期値と最大速度制限バースト設定は 75 パケット / 秒です。
TSPEC Mode	AP の TSPEC モードを設定します。 「On」- AP が「Radio」ページで設定した「TSPEC」のリクエストに対応します。Wi-Fi を利用した電話など QoS 有効の機器からのトラフィックに AP が対応する際など、本機能を有効にします。 「Off」- AP はクライアントステーションなどの TSPEC リクエストを無視します。QoS 有効の機器からのトラフィックなどに限らず、時間順のトラフィック対応をする場合に「Off」に設定します。
TSPEC Voice ACM Mode	音声アクセスに対する TSPEC Voice ACM モードの設定を行います。 「On」- 音声トラフィックを送信 / 受信する前にステーションが帯域の TSPEC リクエストを AP に送信します。 「Off」- ステーションは TSPEC リクエストの有無に限らず、音声優先トラフィックを送信 / 受信することが可能です。
TSPEC Voice ACM Limit	AP によるアクセスゲインのための音声 AC を使用した無線メディアの試行送信のトラフィックの上限を設定します。
TSPEC Video ACM Mode	ビデオアクセスカテゴリにおけ強制アクセス制御の設定を行います。 「On」- ビデオトラフィックを送信 / 受信する前にステーションが帯域の TSPEC リクエストを AP に送信します。 「Off」- ステーションは TSPEC リクエストの有無に限らず、ビデオ優先トラフィックを送信 / 受信することが可能です。
TSPEC Video ACM Limit	AP によるアクセスゲインのためのビデオ AC を使用した無線メディアの試行送信のトラフィックの上限を設定します。
TSPEC AP Inactivity Timeout	AP がアイドル状態のダウンリンク TS を検出し削除するまでの時間を設定します。
TSPEC Station Inactivity Timeout	AP がアイドル状態のアップリンク TS を検出し削除するまでの時間を設定します。
TSPEC Legacy WMM Queue Map Mode	ACM のキュー操作でのレガシートラフィックの混在を許可します。

「Radio」画面を使用して、無線インタフェース 1 と無線インタフェース 2 の両方を設定します。画面上の設定は、「Radio」プルダウンメニューから選択する無線帯域にだけに適用されます。無線帯域の 1 つに設定を行った後に、「Apply」をクリックし、他方の無線帯域を選択して設定します。

Scheduler Configuration（スケジューラの設定）

無線と VAP のスケジューラ設定はスタンドアロン利用時の DWL-x600AP の機能です。無線と VAP のスケジューラ設定は「Manage」の項目から「Scheduler」を選択します。無線と VAP のスケジューラは VAP や無線が管理モードになるまでのインターバル時間に関するルールを設定します。そのため VAP や無線を自動的に有効 / 無効に設定することができます。

本機能は消費電力の削減や無線スケジュールを業務時間のみの稼動に制限してセキュリティ強化するなどために使用します。「一日のうちの限られた時間のみに無線クライアントを VAP にアクセスさせる」、といった使用方法もあります。
ルールの設定項目として、「開始時刻」「終了時刻」「曜日」があります。

ルールには次の項目が設定されている必要があります。

- 曜日（複数日可）
- 開始時刻（分 / 時）
- 終了時刻（分 / 時）

有効なルールのみプロファイルに追加できます。最大 16 個までのルールをグループとして 1 つのスケジューリングプロファイルにまとめることができます。全く同じ時間ルールを 1 つのプロファイルに 2 つ以上設定することはできません。スケジュールとして設定可能な時間単位は分になります DWL-x600AP シリーズは 16 個までのプロファイルを設定する子 t が可能です。

Manage > Scheduler Configuration の順にメニューをクリックし、以下の画面を表示します。

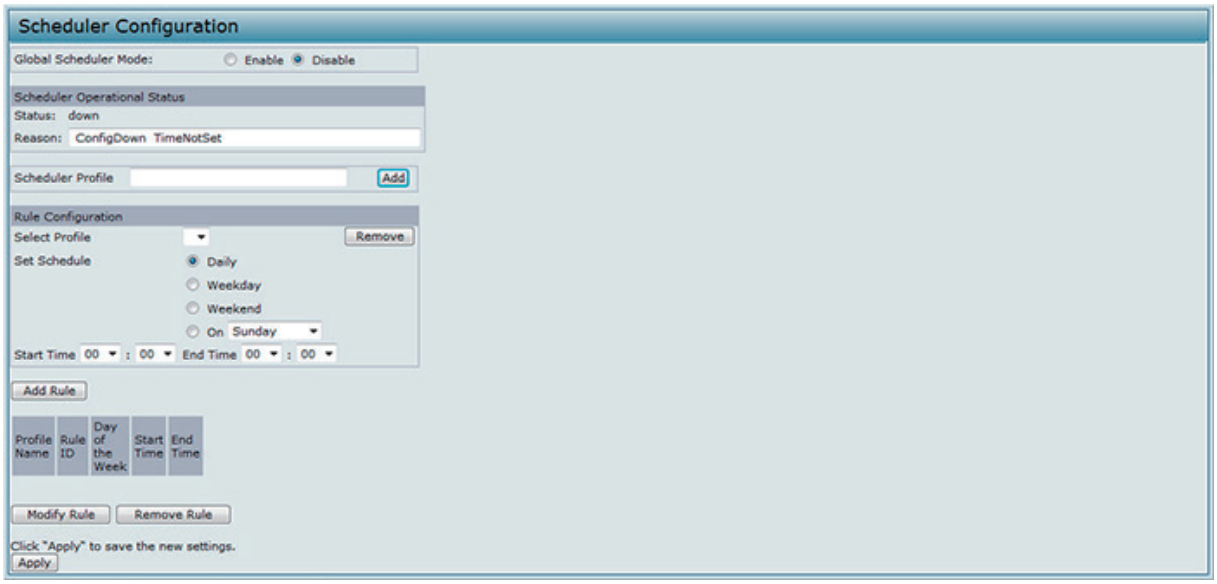


図 5-4　Schedule Config 画面

注意　無線インタフェース設定は、無線インタフェース 1 と無線インタフェース 2 の両方に適用されます。

利用可能な項目と設定オプションについて説明します。

項目	設定内容
Global Scheduler Mode	スケジュール設定をグローバルに有効 / 無効にします。初期値は無効です。
Scheduler Operational Status	
Status	スケジューラの管理ステータスです。範囲は「Up」または「Down」があります。初期値は「Down」です。
Reason	ステータスについての概要です。以下の項目の内、1 つまたは複数選択することが可能です。 「IsActive」- 管理ステータスがアップしています。 「ConfigDown」- グローバルに無効のため、管理ステータスはダウンしています。 「TimeNotSet」- 管理ステータスはダウンです。AP 側の手動または NTP サーバを使用した時間設定がされていません。 「ManagedMode」- 管理ステータスがダウンです。対象の AP が管理モードです。
Scheduler Profile	VAP や無線の設定に関連するプロファイル名のリストです。ルールはは名前の設定されたスケジューラプロファイルに関連します。最大 16 個までのスケジューラプロファイル名を設定できます。初期値ではプロファイルは設定されていません。プロファイル名は 32 英文字まで使用可能で、「Add」をクリックすることで追加できます。
Rule Configuration	各スケジューラは最大 16 までの期間ルールを設定できます。各ルールについては以下で説明があります。
Select Profile	メニューからプロファイル名を選択します。

項目	設定内容
Set Schedule	日を選択します。 曜日、毎日、平日（月 - 金）、週末（土日）、月、火、水、木、金、土、日から選択ができます。 初期値は「Daily」（毎日）です。
Start Time	開始時刻を設定します。無線 /VAP の管理が可能な時間の設定です。 「時時：分分」の 24 時間方式です。<00-24>:<00-59> から設定します。初期値は「00:00」です。
End Time	終了時刻を設定します。無線 /VAP の管理が可能な時間の設定です。 「時時：分分」の 24 時間方式です。<00-24>:<00-59> から設定します。初期値は「00:00」です。

注意 「Rule Configuration」の「Modify Rule」ボタンをクリックして変更を適用し、設定を保存します。

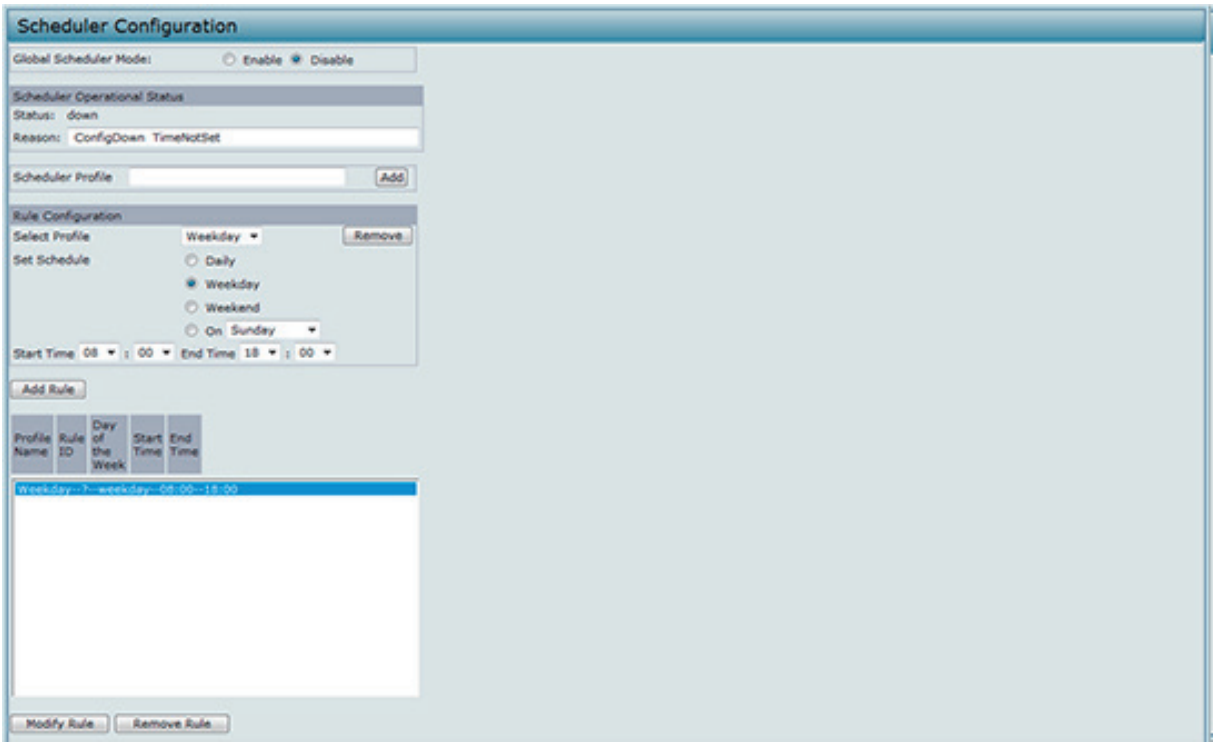


図 5-5　Scheduler Configuration (Modify Rule) 画面

Scheduler Association Settings（スケジューラ関連設定）

スケジューラプロファイルを有効にするためには、少なくとも 1 つ以上の無線または VAP と連携しなければなりません。スケジューラプロファイルを連携させるには「Manage」の「Scheduler Association」をクリックします。初期値ではスケジューラプロファイルは作成されていないため、どの無線、VAP とも連携していません。スケジューラプロファイルは確実に無線または VAP の設定と連携する必要があります。複数の無線または VAP 設定と連携可能なスケジューラプロファイルは 1 つのみです。もし VAP や無線と連携しているスケジューラプロファイルが削除されると、その無線や VAP と連携しているプロファイルはそのうち削除されます。もし無線が無効になると、VAP 設定には関係なく、無線に関連する全ての VAP は無効になります。

Manage > Scheduler Association の順にメニューをクリックし、以下の画面を表示します。

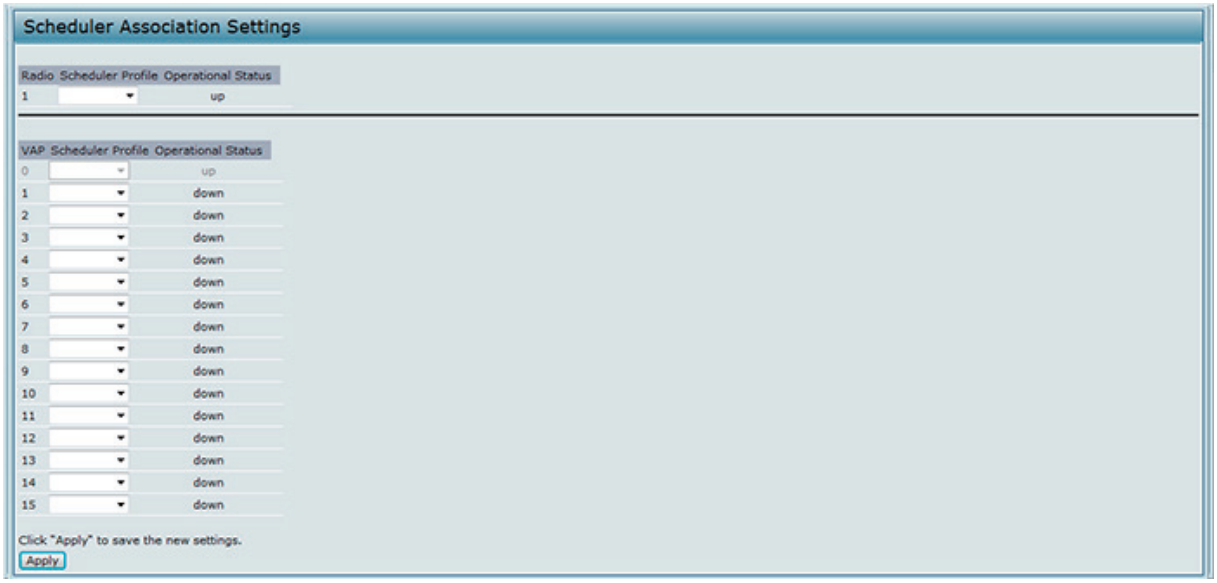


図 5-6　Scheduler Association Settings 画面

利用可能な項目と設定オプションについて説明します。

項目	説明
Radio Scheduler Profile Operational Status	
1 or 2	「Radio 1」または「Radio 2」と連携するスケジューラプロファイルを選択します。
Scheduler Profile	無線と連携しているスケジューラプロファイルを選択します。
Status	スケジューラの管理ステータスです。範囲は「Up」または「Down」です。
VAP Scheduler Profile Operational Status	
Radio	VAP スケジューラプロファイルと連携する「Radio 1」「Radio 2」を選択します。
0-15	それぞれの VAP のスケジューラプロファイルを選択します。
Status	スケジューラの管理ステータスです。範囲は「Up」または「Down」です。

注意　設定を実施後に「Apply」ボタンをクリックして変更を適用して設定を保存します。

VAP（仮想アクセスポイントの設定）

VAP 0 の変更、有効化、および追加の VAP を設定するためには、管理セクションで「VAP」タブを選択します。

イーサネットの VLAN と同様に、無線 LAN は VAP により複数のブロードキャストドメインに分割することができます。VAP は 1 つの物理的なアクセスポイントに複数のアクセスポイントをシミュレートします。各無線帯域は最大 16 個の VAP をサポートしています。

各 VAP に対して、無線クライアントアクセスを制御するためにセキュリティモードをカスタマイズすることができます。また、各 VAP は固有の SSID を持つことができます。複数の SSID は、ただ一つのアクセスポイントをネットワークにある別のシステムに対して 2 つ以上であるように見せます。VAP を設定することで、ブロードキャストやマルチキャストのトラフィック管理が容易になり、ネットワークのパフォーマンスも向上します。

VLAN が同じ無線帯域、または、異なる無線帯域にあっても、異なる VLAN を使用するためには各 VAP の設定、または同じ VLAN を使用するために複数の VAP の設定を行うことができます。VAP0 は、常に両方の帯域で有効であり、デフォルト VLAN1 に割り当てられます。

アクセスポイントは、「VAP」画面で設定する VLAN ID に基づいて、または、RADIUS サーバの割り当てを使用することで無線クライアントトラフィックに VLAN ID タグを追加します。外部の RADIUS サーバを使用する場合、各 VAP で複数の VLAN を設定することができます。外部の RADIUS サーバは、無線クライアントが接続し、認証を行う場合にその無線クライアントを VLAN に割り当てます。

最大 4 つのグローバルな IPv4 または IPv6 RADIUS サーバを設定することができます。サーバの 1 つはプライマリとして常に機能し、一方他のサーバはバックアップサーバとして機能します。ネットワークタイプ（IPv4 または IPv6）とアカウンティングモードは、設定済みのすべての RADIUS サーバを通過するのが一般的です。各 VAP を設定してグローバルな RADIUS サーバの設定を使用することができます。（初期値）また、VAP ごとに異なる RADIUS サーバ設定を行うことも可能です。例えば、ある VAP を設定して、IPv6 RADIUS サーバを使用します。一方、別の VAP ではグローバルな IPv4 RADIUS サーバ設定を使用します。

無線クライアントが RADIUS サーバと通信しないセキュリティモードを使用している場合、または RADIUS サーバが VLAN 情報を提供しない場合、各 VAP に VLAN ID を割り当てることができます。アクセスポイントはその VAP を通じてアクセスポイントに接続するすべての無線クライアントに VLAN を割り当てます。

注意 アクセスポイントに VLAN を設定する前に、アクセスポイントが使用するスイッチと DHCP サーバが、IEEE 802.1Q VLAN のカプセル化をサポートしていることを必ず確認してください。

複数の VAP を設定するためには、**Manage > VAP** の順にメニューをクリックし、以下の画面を表示します。

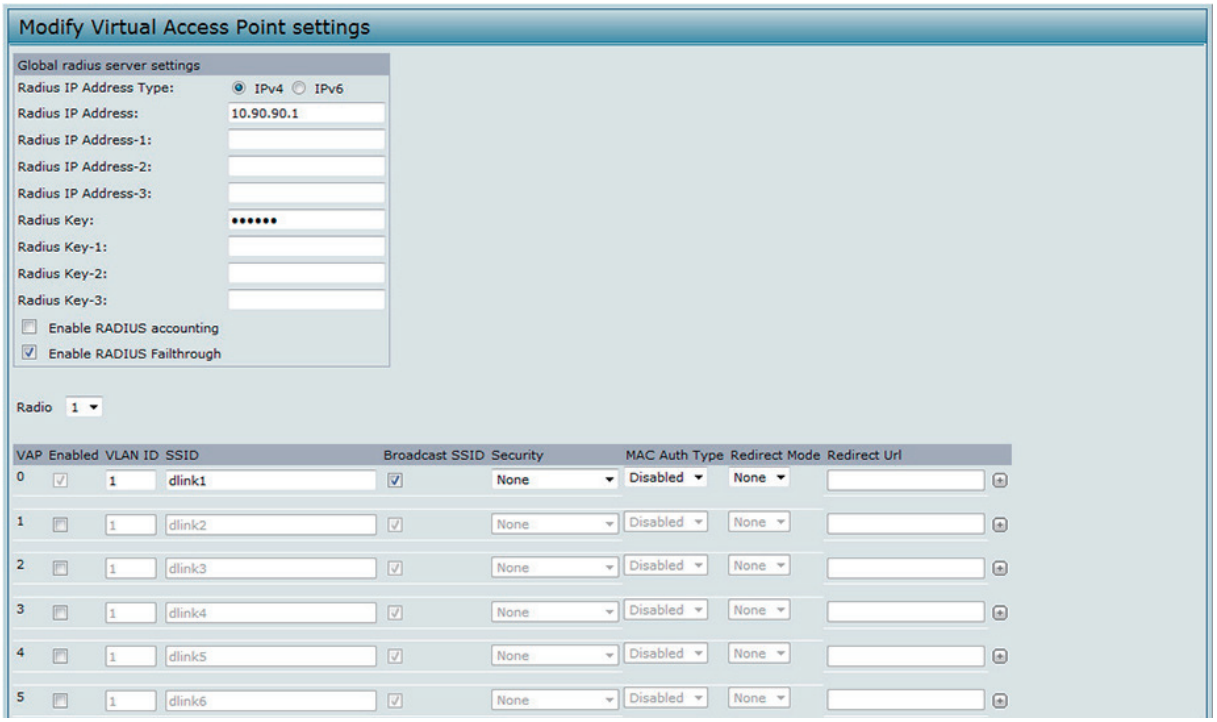


図 5-7　仮想アクセスポイント設定の編集 画面

利用可能な項目と設定オプションについて説明します。

項目	説明
RADIUS IP Address Type	RADIUS サーバが使用する IP バージョン（IPv4 または IPv6）を指定します。 アドレスタイプを切り替えて IPv4 と IPv6 のグローバルな RADIUS アドレスの設定を行いますが、アクセスポイントはこの欄で選択するアドレスタイプの RADIUS サーバまたはサーバだけとコンタクトをとります。
RADIUS IP Address RADIUS IPv6 Address	プライマリグローバル RADIUS サーバの IPv4 または IPv6 アドレスを入力します。初期値では、各 VAP は「VAP」画面の上部でアクセスポイントに定義するグローバルな RADIUS 設定を使用します。 最初の無線クライアントがアクセスポイントに認証を試みる場合、アクセスポイントはプライマリサーバに認証要求を送信します。プライマリサーバが認証要求に応じると、アクセスポイントはプライマリサーバとしてこの RADIUS サーバの使用を継続し、指定するアドレスに認証要求を送信します。 「IPv4 RADIUS IP Address Type」のオプションを前の欄で選択した場合、すべての VAP が初期値で使用する RADIUS サーバの IP アドレス（例 192.168.10.23）を入力します。「IPv6 RADIUS IP Address Type」オプションを選択した場合、プライマリのグローバル RADIUS サーバの IPv6 アドレス（例 2001:0db8:1234::abcd）を入力します。
RADIUS IP Address 1-3 RADIUS IPv6 Address 1-3	バックアップ RADIUS サーバとして使用する最大 3 個の IPv4 または IPv6 アドレスを入力します。「IPv4 RADIUS IP Address Type」オプションを選択すると、項目のラベル名は「IPv4 RADIUS IP Address」となり、「IPv6 RADIUS IP Address Type」オプションの場合には、「IPv6 RADIUS IP Address」となります。 認証がプライマリサーバで失敗すると、設定された各バックアップサーバで順番に行われます。アクセスポイントが、サーバにコンタクトを試みるためには、IPv4 または IPv6 アドレスが有効である必要があります。
RADIUS Key	RADIUS キーを入力します。 RADIUS キーは、グローバル RADIUS サーバ用の共有秘密鍵です。63 文字以内の半角英数字および特殊文字を使用できます。キーは大文字と小文字を区別しており、アクセスポイントと RADIUS サーバに同じキーを設定する必要があります。入力時に周囲からキーを見られないように、入力した文字は "*" で表示されます。
RADIUS Key 1-3	設定済みのバックアップ RADIUS サーバに関連付ける RADIUS キーを入力します。RADIUS IP Address-1 のサーバは RADIUS Key-1、RADIUS IP Address-2 では RADIUS Key-2 というように使用します。
Enable radius accounting	本項目を選択すると、システム時間、送受信したデータ量など、特定のユーザのリソース使用状況を追跡して測定します。RADIUS アカウンティングを有効にすると、プライマリ RADIUS サーバとすべてのバックアップサーバに有効となります。
Enable RADIUS FailThrough	プライマリ RADIUS サーバの認証に失敗した時、セカンダリ RADIUS サーバが無線クライアントの認証を行います。
Radio	設定する無線帯域を選択します。VAP は各無線帯域で個別に設定されます。
VAP	各無線インタフェースに 16 個までの VAP を設定できます。VAP0 が物理的な無線インタフェースであるため、VAP0 を無効にするためには、無線インタフェースを無効にする必要があります。
Enabled	設定したネットワークを「Enabled」（有効）または「Disabled」（無効）にします。特定のネットワークを無効にすると、入力した VLAN ID は失われます。
VLAN ID	無線クライアントがこの VAP を使用してアクセスポイントに接続する場合、タグなし VLAN ID の入力、または RADIUS サーバを使用した無線クライアントの VLAN への割り当てを行わなければ、アクセスポイントは無線クライアントのトラフィックすべてに、ここで入力した VLAN ID をタグ付けします。VLAN ID の範囲は、1-4094 です。 クライアントに RADIUS ベースの認証を使用すると、クライアントに VLAN を設定するために以下の属性をオプションで RADIUS または AAA サーバ内の適切なファイルに追加することができます。 • Tunnel-Type • Tunnel-Medium-Type • Tunnel-Private-Group-ID RADIUS が割り当てた VLAN ID は、「VAP」画面で設定する VLAN ID を上書きします。 「Ethernet Settings」画面でタグなし、管理 VLAN ID を設定します。詳しくは、「Ethernet Settings（イーサネット設定）」（37 ページ）を参照してください。
SSID	無線ネットワーク名を入力します。SSID は、32 文字以内の半角英数字の文字列です。 複数の VAP に同じ SSID を使用することができます。または、各 VAP に固有の SSID を選択することもできます。 **注意** 無線クライアントとして管理しているものと同じアクセスポイントに接続する場合、SSID をリセットすると、アクセスポイントへ接続性を失います。この新しい設定を保存した後に新しい SSID に再接続する必要があります。
Broadcast SSID	アクセスポイントがビーコンフレーム内の SSID をブロードキャストするかどうかを指定します。 初期値では Broadcast SSID は有効です。VAP が SSID をブロードキャストしないと、クライアントステーション上の「使用可能ネットワークリスト」にネットワーク名が表示されなくなります。その代わりに、クライアントは接続前に、サプリカントに接続する相手の正しいネットワーク名を登録する必要があります。 • SSID ブロードキャストを有効にするために、「Broadcast SSID」のチェックボックスを選択します。 • SSID ブロードキャストを無効にするために、「Broadcast SSID」のチェックボックスをクリアします。 **注意** ブロードキャスト SSID を無効にすることで、あるクライアントが偶然ネットワークに入ってくることを防ぐことができます。しかし、ハッカーからの簡単な攻撃を防いだり、暗号化されていないトラフィックを監視するためには十分ではありません。本機能は、ゲストネットワークのような、クライアントからの接続が容易であることに重点を置いた、比較的無防備なネットワークに対して、最低限のレベルの防御を提供するものです。

項目	説明
Security	この VAP に対して以下のセキュリティモードから一つ選択します。 • None • Static WEP • WPA Enterprise • WPA Personal • IEEE 802.1X 「None」以外のセキュリティモードを選択すると、新しい欄が表示されます。これらの欄については以下で説明します。 **注意** ここで設定するセキュリティモードはこの VAP 専用です。
MAC Auth Type	ネットワークへのアクセスを許可または拒否する MAC アドレスのグローバルなリストを設定することができます。 プルダウンメニューで、使用する MAC 認証のタイプを選択します。 • Disabled - MAC 認証をしません。 • Local -「MAC Authentication」画面で設定した MAC 認証リストを使用します。 • Radius - 外部 RADIUS サーバの MAC 認証リストを使用します。 MAC 認証に関する情報については、「MAC Authentication（MAC 認証によるアクセス制御）」（57 ページ）を参照してください。
Redirect Mode	「None」または「HTTP」を選択します。 「HTTP」を選択すると、カスタム Web 画面に無線クライアントをリダイレクトする HTTP リダイレクト機能を有効にします。ユーザは無線クライアントがアクセスポイントに接続し、インターネットにアクセスするために Web ブラウザをオープン後に指定した URL にリダイレクトされます。 カスタム Web 画面は、外部の Web サーバにおかれる必要があり、会社のロゴやネットワーク利用ポリシーなどの情報を含む可能性があります。 **注意** 無線クライアントは一度アクセスポイントに接続すると外部の Web サーバにリダイレクトされます。
Redirect Url	無線クライアントがアクセスポイントに接続し、HTTP トラフィックを送信した後に Web ブラウザがリダイレクトされる URL を指定します。

注意 VAP 設定後に「Apply」ボタンをクリックして変更を適用して設定を保存します。設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

NONE（プレーンテキスト）

「Security」で「None」を選択すると、そのアクセスポイントに対してそれ以上の設定は不必要です。本モードでは、アクセスポイントへの（からの）データ転送には暗号化が行われません。本セキュリティモードは初期のネットワーク設定時、または問題解決時の使用に便利です。しかし、本モードの選択は、安全性が極めて低いため、内部用ネットワークでの通常使用にはお勧めできません。

Static WEP

「Security」で「Static WEP」を選択し、以下の画面を表示します。

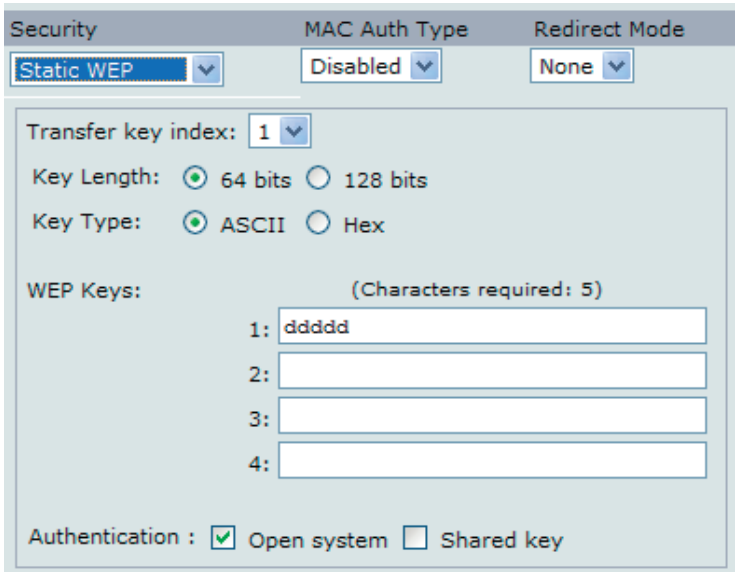


図 5-8　仮想アクセスポイント設定の編集 画面 - Security : Static WEP

WEP（Wired Equivalent Privacy）は 802.11 無線ネットワーク用のデータ暗号化プロトコルです。ネットワーク上のすべての無線クライアントやアクセスポイントは、データの暗号化に 64 ビット（秘密鍵 40 ビット + 初期化ベクタ（IV）24 ビット）、または 128 ビット（秘密鍵 104 ビット +IV 24 ビット）の共有鍵を使用して設定されます。

スタティック WEP は最も安全なモードというわけではありませんが、外部ユーザが暗号化されていない無線トラフィックを探し出すのを防止することは可能であり、セキュリティモードに「None」（プレーンテキスト）を設定するよりもネットワーク保護に役立ちます。

WEP は無線ネットワークを移動するデータはスタティックキーを基に暗号化します（暗号化のアルゴリズムは RC4 と呼ばれるストリーム暗号です）。

画面には以下の項目があります。

項目	説明
Transfer Key index	プルダウンメニューからキーインデックスを選択します。キーインデックス（1-4）が利用可能です。初期値は 1 です。 「Transfer Key Index」（送信キーインデックス）は、アクセスポイントがどの WEP キーを送信するデータの暗号化に使用するかを示します。
Key Length	ラジオボタンで以下の WEP キー長を選択します。 • 64 bits • 128 bits
Key Type	ラジオボタンでどちらかのキー種別を選択します。 • ASCII • Hex
WEP Keys	4 つまでの WEP キーを登録できます。各テキストボックスに、各キーの文字列を入力します。登録するキーはキータイプによって異なります。 • ASCII - アルファベットの大文字、小文字、数字、および @# などの記号を含みます。 • Hex - 0-9 と A-F を含みます。 「要求される文字」で示されるように各キーには同じ文字数を使用します。 これらは RC4 WEP キーでアクセスポイントを使用するステーションと共有します。 各クライアントは、アクセスポイント用に指定したのと同じスロットに、同じ WEP キーから 1 つ登録します。 要求される文字 :「WEP Key」欄に入力する文字数は選択する「Key Length」と「Key Type」によって決定されます。例えば、128 ビットの ASCII キーを使用する場合、WEP キーに 26 文字を入力する必要があります。必要とされる文字数は、「Key Length」と「Key Type」への設定によって自動的に更新されます。
Authentication	認証アルゴリズムは、セキュリティモードがスタティック WEP である場合にクライアントステーションをアクセスポイントに接続するかどうかを決定するのに使用する方法を定義します。 以下のオプションの 1 つを選択し、使用する認証アルゴリズムを指定します。 • Open system - クライアントステーションに正しい WEP キーがあるか否かに関係なく、認証アルゴリズムがこれに設定されると、どんなクライアントステーションもアクセスポイントに接続します。また、本アルゴリズムはプレーンテキスト、IEEE 802.1X、および WPA モードで使用されます。 **注意** クライアントステーションが接続を許可されているだけであり、アクセスポイントとのトラフィックの交換を保証するものではありません。ステーションは、アクセスポイントからのデータへのアクセスと解読に成功し、アクセスポイントに読み込み可能であるデータを送信するためには正しい WEP を持つ必要があります。 • Shared Key - クライアントステーションがアクセスポイントに接続するためには、正しい WEP キーを持つことが必要です。認証アルゴリズムが Shared Key に設定されると、不正な WEP キーを持つステーションはアクセスポイントに接続することはできません。 • Both Open System と Shared Key の両方を選択 - 両方の認証アルゴリズムを選択する場合、以下の通りとなります。 - Shared Key モードで WEP を使用するように設定されたクライアントステーションは、アクセスポイントに接続するために有効な WEP キーを持つ必要があります。 - WEP を Open System（Shared Key モードは無効）として使用するように設定されたクライアントステーションはそれらに正しい WEP キーを持たなくてもアクセスポイントに接続することができます。

スタティック WEP ルール

スタティック WEP を使用する際は、以下のルールが適用されます。

- すべてのクライアントは WLAN セキュリティを「WEP」に設定し、アクセスポイントからクライアントへの送信データを復号するために、アクセスポイントで指定されている WEP キーのうちの 1 つを持つ必要があります。
- アクセスポイントは、クライアント側からのデータを復号するために、クライアントがアクセスポイントへの送信に使用するすべてのキーを持つ必要があります。
- すべてのノード（アクセスポイントとクライアント）では、キーは同じスロットを使用します。例えばアクセスポイントが「abc123」キーを WEP キー 3 と定義したならば、クライアント側も同じキーを WEP キー 3 と定義する必要があります。
- クライアントは、アクセスポイントへのデータ送信用にそれぞれ異なるキーを使用できます。複数のクライアントが同じキーを使用することもできますが、その場合は他のクライアントからのデータを解読できるため、安全性は低くなります。
- 無線クライアントソフトウェアによっては、複数の WEP キーを登録し、" 送信キーインデックス " を定義し、異なるキーを切り替えてデータを暗号化するように設定をすることもできます。これにより、近接するアクセスポイントがお互いの通信内容を解読できなくなります。
- アクセスポイントとクライアントステーション間で、64 ビットおよび 128 ビットの WEP キーを混在させることはできません。

IEEE 802.1X

「Security」で「IEEE 802.1X」を選択し、以下の画面を表示します。

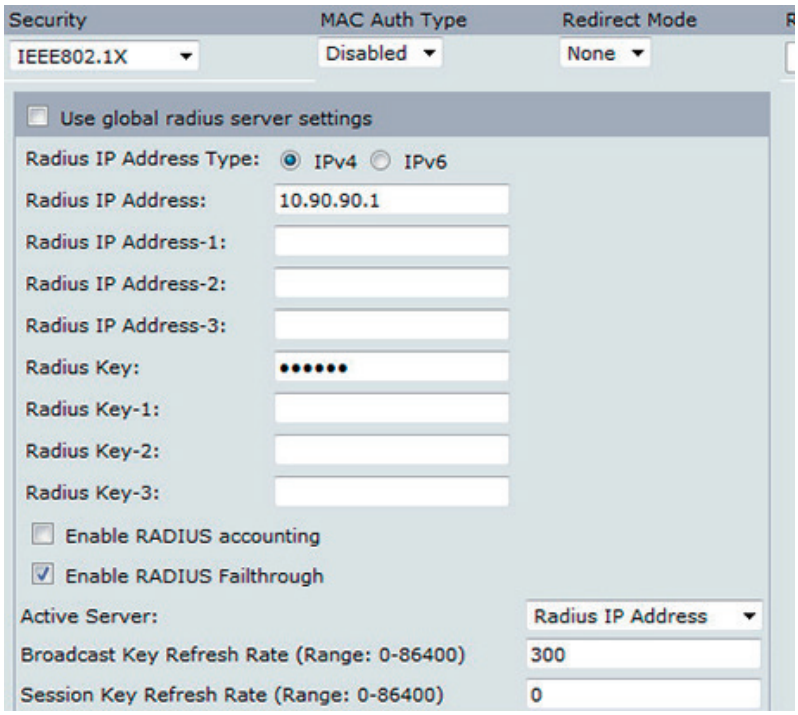


図 5-9　仮想アクセスポイント設定の編集 画面 - Security : IEEE 802.1X

IEEE 802.1X はポートベース認証を定義する規格で、キー管理をするための基本的なアーキテクチャです。Extensible Authentication Protocol（EAP）メッセージは、EAP Encapsulation Over LANs（EAPOL）と呼ばれるプロトコルを使用することで IEEE 802.11 無線ネットワークに送信されます。IEEE 802.1X はダイナミックに生成されるキーを提供し、これは定期的に更新されます。RC4 ストリーム暗号は、各 802.11 フレームの本体と CRC（巡回冗長検査）を暗号化するために使用されます。

本モードでは、ユーザを認証するために外部の RADIUS サーバの使用を必要とします。アクセスポイントは、マイクロソフトインターネット認証サーバなど EAP が有効な RADIUS サーバを必要とします。Windows クライアントと共に動作するためには、認証サーバは Protected EAP（PEAP）および MS-CHAP V2 をサポートする必要があります。

証明書、ケルベロス、および公開鍵認証を含む IEEE 802.1X モードがサポートする様々な認証方法のいずれかを使用することができます。クライアントステーションを、アクセスポイントが使用するのと同じ認証方法を使用するように設定する必要があります。

項目	説明
Use global radius server settings	初期値では、各 VAP は「VAP」画面の上部でアクセスポイントに定義するグローバルな RADIUS 設定を使用します。しかし、異なる RADIUS サーバのセットを使用するためには各 VAP を設定します。 グローバルな RADIUS サーバ設定を使用するためには、チェックボックスが選択されていることを確認してください。 VAP に個別の RADIUS サーバを使用するためには、チェックボックスのチェックを外し、以下の欄に RADIUS サーバの IP アドレスを入力してください。
Radius IP Address Type	RADIUS サーバが使用する IP バージョン（IPv4 または IPv6）を指定します。 アドレスタイプを切り替えて IPv4 と IPv6 のグローバルな RADIUS アドレスの設定を行いますが、アクセスポイントはこの欄で選択するアドレスタイプの RADIUS サーバまたはサーバだけとコンタクトをとります。
Radius IP Address / Radius IPv6 Address	この VAP に対してプライマリ RADIUS サーバの IPv4 または IPv6 アドレスを入力します。 「Radius IP Address Type」のオプションで「IPv4 」を選択した場合、すべての VAP が初期値で使用する RADIUS サーバの IP アドレス（例 192.168.10.23）を入力します。「Radius IP Address Type」オプションで「IPv6」を選択した場合、プライマリのグローバル RADIUS サーバの IPv6 アドレス（例 2001:0db8:1234::abcd）を入力します。
Radius IP Address 1-3 / IPv6 IP Address 1-3	バックアップ RADIUS サーバとして使用する最大 3 個の IPv4 または IPv6 アドレスを入力します。「Radius IP Address Type」オプションで「IPv4」を選択すると、項目のラベル名は「IPv4 Radius IP Address」となり、「Radius IP Address Type」オプションで「IPv6」を選択すると「IPv6 Radius IP Address」となります。 認証がプライマリサーバで失敗すると、設定された各バックアップサーバで順番に行われます。
Radius Key	テキストボックスに RADIUS キーを入力します。 RADIUS キーは、グローバル RADIUS サーバ用の共有秘密鍵です。63 文字以内の半角英数字および特殊文字を使用できます。キーは大文字と小文字を区別しており、アクセスポイントと RADIUS サーバに同じキーを設定する必要があります。入力時に周囲からキーを見られないように、入力した文字は "*" で表示されます。
Radius Key 1-3	設定済みのバックアップ RADIUS サーバに関連付ける RADIUS キーを入力します。「Radius IP Address-1」のサーバは「Radius Key-1」、「Radius IP Address-2」では「Radius Key-2」というように使用します。
Enable Radius accounting	本オプションを選択すると、システム時間、送受信したデータ量など、特定のユーザのリソース使用状況を追跡して測定します。 RADIUS アカウンティングを有効にすると、プライマリ RADIUS サーバとすべてのバックアップサーバに有効となります。
Enable RADIUS FailThrough	プライマリ RADIUS サーバの認証に失敗した時、セカンダリ RADIUS サーバが無線クライアントの認証を行います。
Active Server	アクティブにする RADIUS サーバ（Radius IP Address、Radius IP Address-1、Radius IP Address-2、Radius IP Address-3）を選択します。
Broadcast Key Refresh Rate	この VAP に接続するクライアントが使用するブロードキャスト（グループ）キーの更新間隔時間を入力します。 範囲は 0-86400（秒）です。0 は、ブロードキャストキーが更新されないことを示します。
Session Key Refresh Rate	この VAP に接続する各クライアントが使用するセッション（ユニキャスト）キーの更新間隔時間を入力します。 範囲は 0-86400（秒）です。0 は、ブロードキャストキーが更新されないことを示します。

注意 セキュリティ設定を実施後に「Apply」ボタンをクリックして変更を適用して設定を保存します。

WPA Personal

「Security」で「WPA Personal」を選択し、以下の画面を表示します。

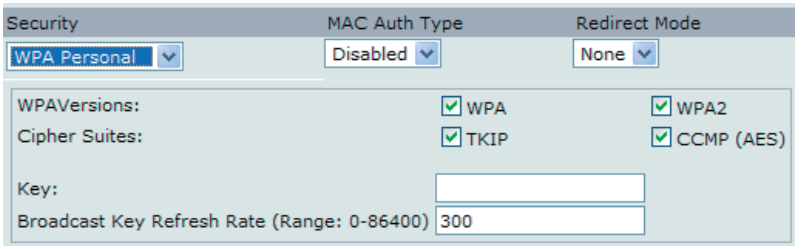


図 5-10　仮想アクセスポイント設定の編集 画面 - Security : WPA Personal

WPA Personal は Wi-Fi Alliance により発表された IEEE 802.11i の規格で、AES-CCMP および TKIP というメカニズムを採用しています。WPA Personal は WPA Enterprise で使用する「IEEE 802.1X」や「EAP」の代わりに、「pre-shared key」(事前共有鍵) を使用します。PSK は証明書の初期チェックだけに使用されます。

このセキュリティモードは、オリジナルの WPA をサポートする無線クライアントと下位互換性を持っています。

項目	説明
WPA Versions	サポートするクライアントステーションの WPA のタイプを選択します。 • WPA - ネットワーク上のすべてのクライアントが WPA をサポートし、WPA2 をサポートしていない場合は、WPA を選択します。 • WPA2 - ネットワーク上のすべてのクライアントが WPA2 をサポートしている場合は、IEEE 802.11i 規格で最も安全なセキュリティを提供する WPA2 を使用することをお勧めします。 • WPA and WPA2 - WPA と WPA2 をサポートするクライアントが混在している場合は、両方のボックスを選択します。サポートする方式に関わらずクライアント間の接続および認証が行えます。ただし、WPA2 サポートのクライアントに対しては、多少セキュリティは高くなります。本設定では相互運用性を実現する代わりに、セキュリティを若干低くしています。
Cipher Suites	使用する暗号化方式を選択します。 • TKIP • CCMP（AES） • TKIP と CCMP（AES） TKIP と AES サポートのクライアントのどちらも、アクセスポイントへの接続が可能です。アクセスポイントとの接続のために、WPA クライアントは以下のどちらかを持っている必要があります。 • 有効な TKIP キー • 有効な AES-CCMP キー WPA パーソナルを使用するように設定されていないクライアントは、アクセスポイントに接続することはできません。
Key	Pre-shared Key は、WPA パーソナルで使用する共有秘密鍵です。8 から 63 の半角英数字を入力します。アルファベットの大文字、小文字、数字、および @# などの記号が入力できます。
Broadcast Key Refresh Rate	この VAP に接続するクライアントが使用するブロードキャスト（グループ）キーの更新間隔時間を入力します。 範囲は 0-86400（秒）です。0 は、ブロードキャストキーが更新されないことを示します。

WPA Enterprise

「Security」で「WPA Enterprise」を選択し、以下の画面を表示します。

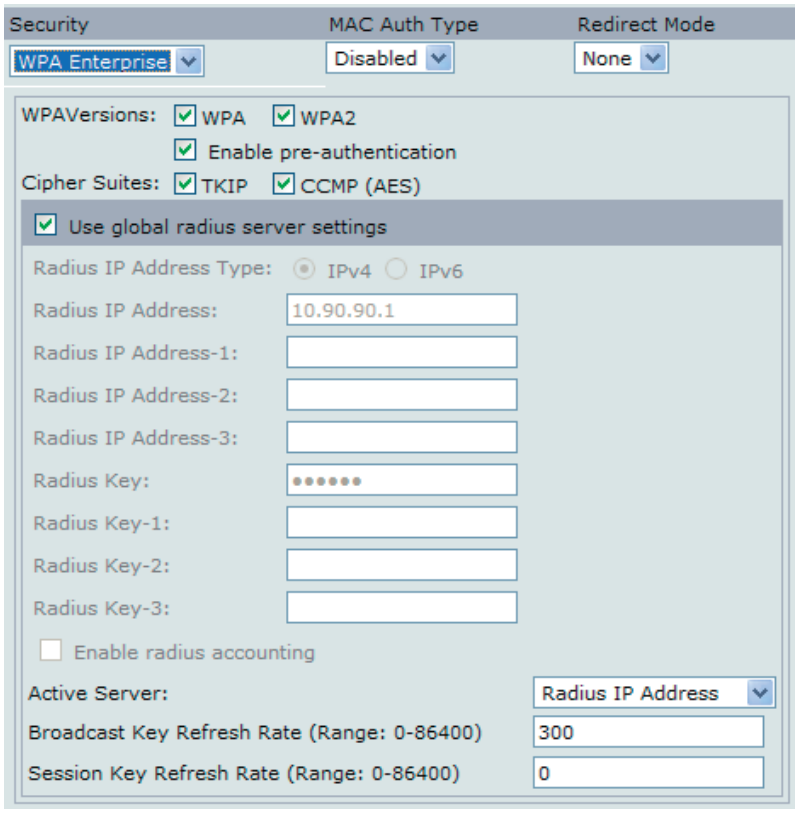


図 5-11　仮想アクセスポイント設定の編集 画面 - Security : WPA Enterprise

RADIUS と共に WPA Enterprise は Wi-Fi Alliance の IEEE 802.11i 標準に準拠した規格で、CCMP（AES）および TKIP というメカニズムを採用しています。Enterprise モードでは、ユーザを認証するために RADIUS サーバの使用を必要とします。

このセキュリティモードはオリジナルの WPA をサポートする無線クライアントと下位互換性があります。

項目	説明
WPA Versions	サポートするクライアントステーションの WPA のタイプを選択します。 • WPA - ネットワーク上のすべてのクライアントが WPA をサポートし、WPA2 をサポートしていない場合は、WPA を選択します。 • WPA2 - ネットワーク上のすべてのクライアントステーションが WPA2 をサポートしている場合は、IEEE 802.11i で最も安全なセキュリティを提供する WPA2 を使用することをお勧めします。 • WPA と WPA2 - WPA と WPA2 をサポートするクライアントが混在している場合は、両方のボックスを選択します。サポートする方式に関わらずクライアント間の接続および認証が行えます。ただし、WPA2 サポートのクライアントに対しては、多少セキュリティは高くなります。本設定では相互運用性を実現する代わりに、セキュリティを若干低くしています。
Enable pre-authentication	WPA バージョンに WPA2、または WPA2 と WPA の両方を選択すると、WPA2 クライアントに対して事前認証を有効にすることができます。 WAP2 対応の無線クライアントから事前認証パケットを送信する場合は「Pre-Authentication」チェックボックスにチェックを入れます。事前認証情報はクライアントが接続中のアクセスポイントから、送信先のアクセスポイントに受け渡されます。本機能を有効にすると、複数のアクセスポイントと接続するローミングクライアントの認証を高速化することができます。 従来の WPA は本機能をサポートしていないため、「WPA Versions」に WPA を選択すると、本オプションは適用されません。
Cipher Suites	使用する暗号化方式を選択します。 • TKIP • CCMP（AES） • TKIP と CCMP（AES） 初期値では、TKIP と CCMP の両方が選択されます。TKIP と CCMP の両方が選択される場合、RADIUS を持つ WPA を使用するために設定されたクライアントステーションは、以下の 1 つを持つ必要があります。 • 有効な TKIP RADIUS IP アドレスと RADIUS キー • 有効な CCMP (AES) IP アドレスと RADIUS キー
Use global radius server settings	初期値では、各 VAP は「VAP」画面の上部でアクセスポイントに定義するグローバルな RADIUS 設定を使用します。しかし、異なる RADIUS サーバのセットを使用するためには各 VAP を設定します。 グローバルな RADIUS サーバ設定を使用するためには、チェックボックスが選択されていることを確認してください。 VAP に個別の RADIUS サーバを使用するためには、チェックボックスのチェックを外し、本欄に RADIUS サーバの IP アドレスを入力してください。
Radius IP Address Type	RADIUS サーバが使用する IP バージョン（IPv4 または IPv6）を指定します。 アドレスタイプを切り替えて IPv4 と IPv6 のグローバルな RADIUS アドレスの設定を行いますが、アクセスポイントはこの欄で選択するアドレスタイプの RADIUS サーバまたはサーバだけとコンタクトをとります。
Radius IP Address / Radius IPv6 Address	この VAP に対してプライマリ RADIUS サーバの IPv4 または IPv6 アドレスを入力します。 「Radius IP Address Type」オプションで「IPv4」で選択した場合、すべての VAP が初期値で使用する RADIUS サーバの IP アドレス（例 192.168.10.23）を入力します。「Radius IP Address Type」オプションで「IPv6」を選択した場合、プライマリのグローバル RADIUS サーバの IPv6 アドレス（例 2001:0db8:1234::abcd）を入力します。
Radius IP Address 1-3 / Radius IPv6 Address 1-3	バックアップ RADIUS サーバとして使用する最大 3 個の IPv4 または IPv6 アドレスを入力します。「Radius IP Address Type」オプションで「IPv4」を選択すると、項目のラベル名は「IPv4 Radius IP Address」となり、「Radius IP Address Type」オプションで「IPv6」を選択した場合には、「IPv6 Radius IP Address」となります。 認証がプライマリサーバで失敗すると、設定された各バックアップサーバで順番に行われます。
Radius Key	テキストボックスに RADIUS キーを入力します。 RADIUS キーは、グローバル RADIUS サーバ用の共有秘密鍵です。63 文字以内の半角英数字および特殊文字を使用できます。キーは大文字と小文字を区別しており、アクセスポイントと RADIUS サーバに同じキーを設定する必要があります。 入力時に周囲からキーを見られないように、入力した文字は "*" で表示されます。
Radius Key 1-3	設定済みのバックアップ RADIUS サーバに関連付ける RADIUS キーを入力します。「Radius IP Address-1」のサーバは「Radius Key-1」、「Radius IP Address-2」では「Radius Key-2」というように使用します。
Enable Radius Accounting	本オプションを選択すると、システム時間、送受信したデータ量など、特定のユーザのリソース使用状況を追跡して測定します。 RADIUS アカウンティングを有効にすると、プライマリ RADIUS サーバとすべてのバックアップサーバに有効となります。
Enable RADIUS FailThrough	プライマリ RADIUS サーバの認証に失敗した時、セカンダリ RADIUS サーバが無線クライアントの認証を行います。
Active Server	アクティブにする RADIUS サーバ（Radius IP Address、Radius IP Address-1、Radius IP Address-2、Radius IP Address-3）を選択します。
Broadcast Key Refresh Rate	この VAP に接続するクライアントが使用するブロードキャスト（グループ）キーの更新間隔時間を入力します。 範囲は 0-86400（秒）です。0 は、ブロードキャストキーが更新されないことを示します。
Session Key Refresh Rate	この VAP に接続する各クライアントが使用するセッション（ユニキャスト）キーの更新間隔時間を入力します。 範囲は 0-86400（秒）です。0 は、ブロードキャストキーが更新されないことを示します。

WDS（WDS の設定）

WDS（Wireless Distribution System）により複数の本製品への接続が可能となります。WDS を使用して、アクセスポイント同士は標準化された方法でケーブルを使用せずに通信します。この機能はクライアントのローミングや複数の無線ネットワークの管理をシームレスに行うために重要です。また、必要とされるケーブル接続の量を削減することでネットワーク構造を簡素化できます。接続するリンク数に基づいてポイントツーポイントまたはポイントツーマルチポイントのブリッジモードでアクセスポイントを設定することができます。

ポイントツーポイントモードでは、アクセスポイントは、クライアントの接続を許可して無線クライアントや他のリピータと通信を行います。アクセスポイントは、アクセスポイント間で確立されるトンネルを経由する他のネットワークに向けてすべてのトラフィックを転送します。ブリッジはホップ回数に加えません。これは、簡単な OSI のレイヤ 2 ネットワークデバイスとして機能します。

ポイントツーマルチポイントブリッジモードでは、1 つのアクセスポイントが複数のアクセスポイント間で通常のリンクとして機能します。このモードでは、中央のアクセスポイントは、クライアントの接続を許可して無線クライアントや他のリピータと通信を行います。他のアクセスポイントのすべてが、ルーティングの目的のために適切な無線ブリッジにパケットを送信する中央のアクセスポイントとだけ接続します。

本製品はリピータとしても機能できます。本モードでは、アクセスポイントはセル範囲から極めて遠い 2 つのアクセスポイント間を接続します。リピータとして機能する場合、アクセスポイントは、LAN との有線接続は行わず、無線接続を使用することで信号を中継します。アクセスポイントがリピータとして機能するために特別な設定は必要ではなく、リピータモード設定もありません。無線クライアントはリピータとして動作しているアクセスポイントに接続することができます。

注意 AP をスタンドアロンモードから管理モードまで移行させると、WDS は無効になります。管理モードでは、D-Link 統合スイッチを使用することによって、アクセスポイントを設定します。アクセスポイントが管理モードにある場合、Web マネージャ、Telnet、SSH、および SNMP アクセスは無効となります。

このアクセスポイントから他のアクセスポイントまでのトラフィック交換の詳細を指定します。

Manage > WDS の順にメニューをクリックし、以下の画面を表示します。

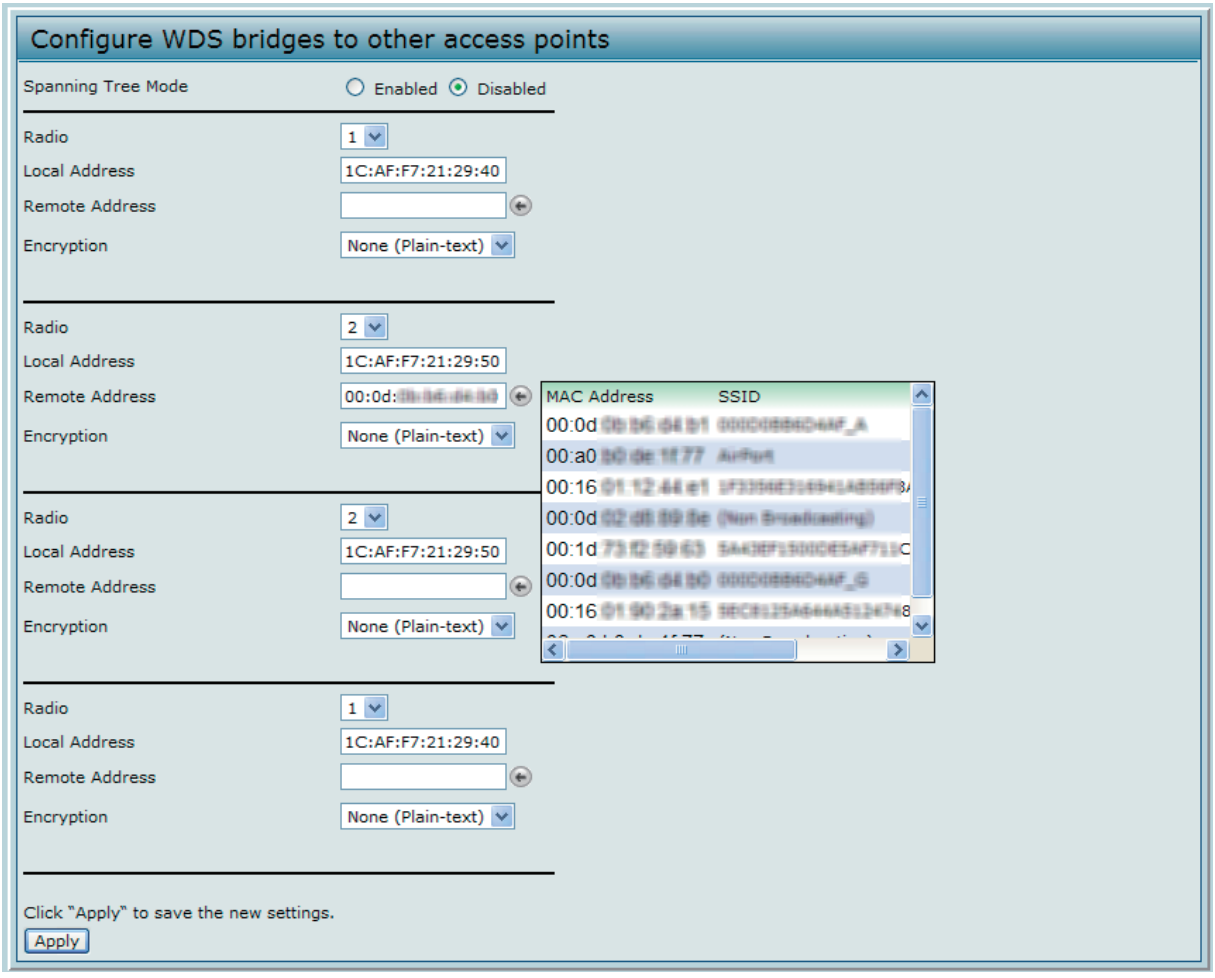


図 5-12　他のアクセスポイントへの WDS ブリッジの設定 画面

アクセスポイントに WDS を設定する前に、以下のガイドラインに注意してください。

- WDS を使用する時には WDS リンクに参加する両方のアクセスポイントに WDS 設定を行ってください。
- アクセスポイントのペア間に WDS リンクだけを持つことができます。つまり、リモート MAC アドレスは特定のアクセスポイントの WDS 画面に一度だけ表示される可能性があります。
- WDS リンクに参加する両方のアクセスポイントが、同じ無線チャンネルにあり、同じ IEEE 802.11 モードを使用する必要があります。（無線モードとチャンネルの設定に関する情報については、「Radio（無線の詳細設定）」（59 ページ）を参照してください。）
- 802.11h が操作可能である場合、2 つの WDS リンクの設定が難しい場合があります。「802.11h 無線モードの使用」（58 ページ）を参照してください。
- 無線 1 を経由した WDS リンクで WPA 暗号化を使用する場合、無線 1 の VAP0 はセキュリティモードとして WPA Personal または WPA Enterprise を使用する必要があります。無線 2 を経由した WDS リンクで WPA 暗号化を使用する場合、無線 2 の VAP0 はセキュリティモードとして WPA Personal または WPA Enterprise を使用する必要があります。

この AP に WDS を設定するために、ハンドオフを受信し、このアクセスポイントに情報を送信する予定の各アクセスポイントについて記載します。各送信先アクセスポイントのために、以下の表に示す項目を設定します。

項目	説明
Spanning Tree Mode	スパニングツリープロトコル（STP）は、スイッチングのループを防ぎます。STP は、WDS リンクを設定する場合に推奨されます。 STP を使用するためには「Enabled」を選択します。 「Disabled」が選択されると STP リンクはオフになります。（推奨されません。）
Radio	２つの無線帯域を持つアクセスポイントにおける各 WDS リンクに対して、「1」または「2」を選択します。リンクの設定の残りはここで選択する無線帯域に適用されます。本欄で選択する「Radio」によって、参照用の「Local Address」は変わります。
Local Address	本アクセスポイントの MAC アドレスを示します。 ２つの無線帯域を持つアクセスポイントの各 WDS リンクに対して、「Local Address」は選択された無線帯域（wlan0 では Radio 1、または wlan1 では Radio 2）上の内部インタフェースの MAC アドレスを反映します。
Remote Address	送信先アクセスポイントの MAC アドレスを指定します。つまり、データが送信またはハンドオフされ、データが受信される WDS リンクの他方の端にあるアクセスポイントです。 「Remote Address」欄の をクリックすると、ネットワークにおけるすべての利用可能な MAC アドレスとそれらに関連する SSID のリストを参照することができます。リストから適切なアクセスポイントの MAC アドレスを選択します。 **注意** リストで表示される SSID は、送信先アクセスポイントの正しい MAC アドレスを特定するために役立ちます。この SSID は WDS リンクに設定するものとは別の SSID です。2 つを同じ値または名前にするべきではありません。
Encryption	WDS リンクで使用する暗号化のタイプ（「Non（Plain - text）」、「WEP」、または「WPA（PSK）」）を指定します。 WDS リンクのセキュリティ問題について気にかけない場合は、「Non（Plain - text）」（暗号化なし）のタイプを選択します。セキュリティの懸念がある場合は、「Static WEP」、または「WPA（PSK）」を選択することができます。WPA（PSK）モードでは、アクセスポイントは WDS リンクに CCMP（AES）準拠の WPA2-PSK 暗号化を使用します。 **注意** どのような WDS リンクでも WPA-PSK を設定するためには、選択した無線帯域の VAP0 が WPA-PSK または WPA-Enterprise に設定される必要があります。

希望する WDS 暗号化オプションとして「None」を選択すると、「WDS」画面でそれ以上の欄への入力は問われません。
WDS リンクにある 2 つのアクセスポイント間に転送されるすべてのデータが、復号化されます。

注意 WDS リンクを無効にするためには、「Remote Address」欄に設定した値を削除する必要があります。

WDS リンクにおける WEP

「Encryption」に「WEP」を選択すると、以下の項目が画面に表示されます。

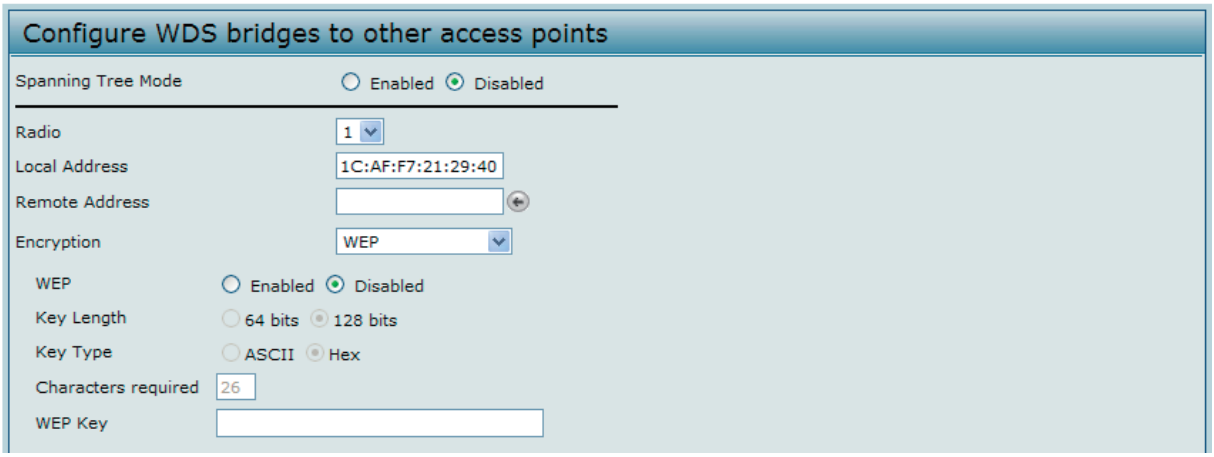


図 5-13　他のアクセスポイントへの WDS ブリッジの設定 画面 - Encryption : WEP

以下の表では、暗号化タイプとして WEP を選択する場合に表示される追加欄について説明します。

項目	説明
Encryption	WEP
WEP	WDS リンクに WEP 暗号化を設定する場合に、本オプションを選択します。
Key Length	WEP を有効にした場合に、WEP キー長を指定します。 • 64 bits • 128 bits
Key Type	WEP を有効した場合に、WEP のキータイプを指定します。 • ASCII • Hex
Characters Required	WEP キーに必要とされる文字数を指定します。 必要とされる文字数は、「Key Length」と「Key Type」への設定によって自動的に更新されます。
WEP Key	文字列を入力します。「ASCII」を選択した場合、半角英数字の組合せを入力します。「HEX」を選択した場合、16 進数（0-9、a-f、または A-F の組合せ）を入力します。これらは RC4 暗号化でアクセスポイントを使用するステーションと共有します。

WDS リンクにおける WPA (PSK)

「Encryption」に「WPA (PSK)」を選択すると、以下の項目が画面に表示されます。

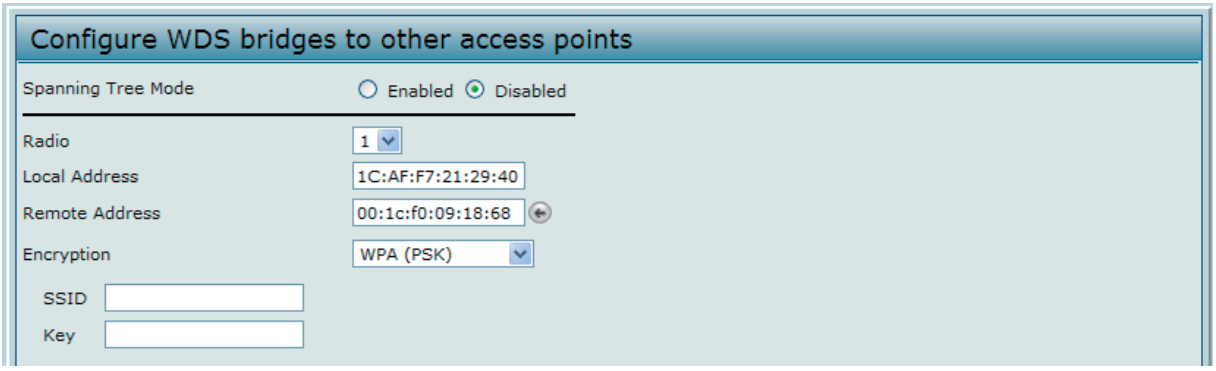


図 5-14　他のアクセスポイントへの WDS ブリッジの設定 画面 - Encryption : WPA (PSK)

以下の表では、暗号化タイプとして WPA (PSK) を選択した場合に表示される追加欄について説明します。

注意 どの WDS リンクでも WPA (PSK) の設定のためには、選択した無線帯域の VAP0 が WPA-PSK または WPA-Enterprise に設定される必要があります。

以下の項目を設定します。

項目	説明
Encryption	WPA（PSK）
SSID	作成した新しい WDS リンクに適切な名称を入力します。この SSID はこのアクセスポイントが使用する別の SSID と異なる必要があります。しかし、同じ SSID が WDS リンクのもう一端にも入力されることが重要です。この SSID が WDS リンク上の両方のアクセスポイントで同じでないと、それらは通信およびデータ交換を行うことはできません。 SSID はあやゆる英数字の組合せで指定することができます。
Key	WDS ブリッジに固有の共有キーを入力します。また、WDS リンクのもう一端のアクセスポイントにもこの固有の共有キーを入力する必要があります。このキーが両方のアクセスポイントで同じでないと、それらは通信およびデータ交換を行うことはできません。 WPA-PSK キーは、8 文字以上 63 文字以下の半角英数字の文字列です。アルファベットの大文字、小文字、数字、および @# などの記号が入力できます。

注意 WDS 設定を実施後に「Apply」ボタンをクリックして変更を適用して設定を保存します。設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

MAC Authentication（MAC 認証によるアクセス制御）

Media Access Control（MAC）アドレスは、ネットワーク上の各ノードを特定するハードウェアアドレスです。すべての IEEE 802 ネットワークデバイスは、一般的な 48 ビットの MAC アドレス形式を共有します。通常、「:」（コロン）で区切られた 12 個の 16 進数（例 00:DC:BA:09:87:65）として表されます。無線クライアントによって使用される各無線ネットワークインタフェースカード（NIC）は、固有の MAC アドレスを持っています。

無線クライアントの MAC アドレスに基づいてアクセスポイント経由でネットワークへのアクセスを制御するために、アクセスポイントの Web マネージャを使用するか、または外部の RADIUS サーバを使用することができます。本機能は、MAC 認証または MAC フィルタリングと呼ばれます。アクセスを制御するためには、アクセスポイント上、または、外部 RADIUS サーバ上に MAC アドレスのグローバルなリストをローカルに設定します。これらの MAC アドレスを持つクライアントネットワークへのアクセスを許可または拒否するかどうかを指定するフィルタを設定することができます。無線クライアントが、アクセスポイントへの接続を試みる場合、アクセスポイントはローカルな「Stations List」にあるクライアントまたは RADIUS サーバ上のクライアントの MAC アドレスを検索します。それが見つけられると、グローバルな許可または拒否設定が適用されます。見つけられないと、その反対が適用されます。

「VAP」画面における「MAC Authentication Type」設定ではアクセスポイントが「MAC Authentication」画面または RADIUS サーバにローカルに設定されているステーションリストを使用するかどうかを制御します。「MAC Authentication」画面の「Allow/Block」設定は、ステーションリスト（local または RADIUS）内のクライアントがアクセスポイントを通じてネットワークにアクセスできるかどうかを決定します。MAC 認証タイプの設定についての詳しい情報は「VAP（仮想アクセスポイントの設定」（66 ページ）を参照してください。

アクセスポイントに MAC フィルタとステーションを設定する

MAC アドレスに基づいたアクセスポイントへのアクセス制御を行います。フィルタの設定方法に基づいて、リストにある MAC アドレスを持つクライアントステーションだけを許可するか、またはリストにあるステーションへのアクセスを拒否することができます。

「MAC Authentication」を有効にして、承認する MAC アドレスのリストを指定する場合、リストにある MAC アドレスを持つクライアントだけがネットワークにアクセスできます。拒否する MAC アドレスを指定する場合、すべてのクライアントが拒否リストにあるクライアントを除いて、ネットワークにアクセスすることができます。

MAC アドレスによるフィルタリングを有効にします。

Manage > MAC Authentication の順にメニューをクリックし、以下の画面を表示します。。

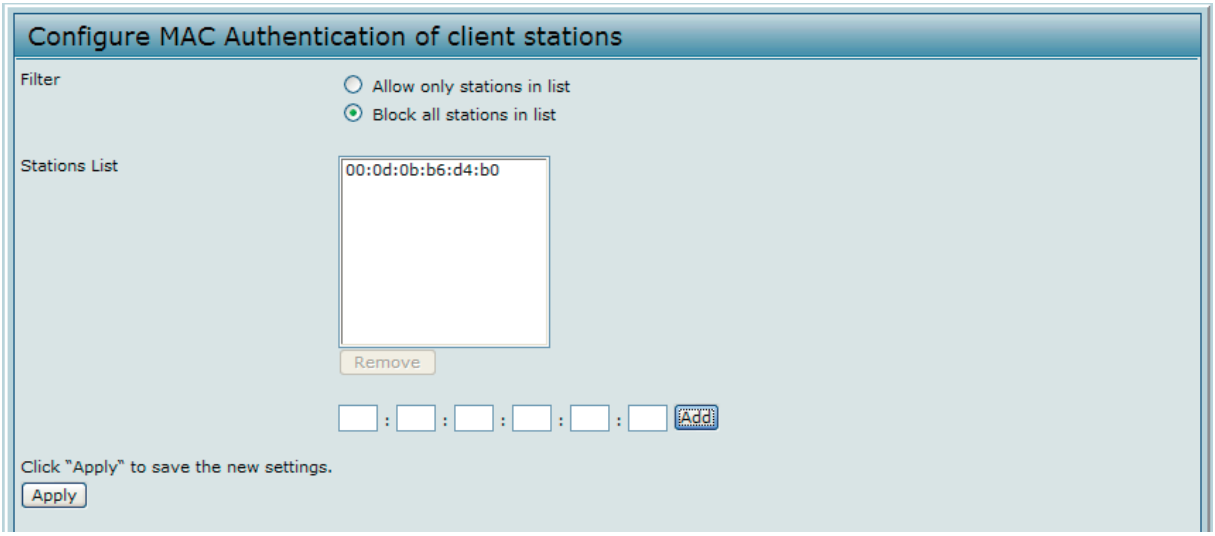


図 5-15　クライアントステーションの MAC 認証設定 画面

注意　グローバルな MAC 認証設定は両方の無線帯域にあるすべての VAP に適用されます。

以下の表では、画面で利用可能な項目と設定オプションについて説明します。

項目	説明
Filter	MAC アドレスフィルタを設定するためには、以下のオプションの 1 つを選択します。 • Allow only stations in list -「Stations List」内にないステーションは、いずれもアクセスポイントを通じたネットワークへのアクセスを拒否されます。 • Block all stations in list - リストにあるステーションだけが、アクセスポイントを通じたネットワークへのアクセスを拒否されます。他のすべてのステーションがアクセスを許可されます。 **注意** 選択するフィルタは、ステーションのリストがローカルまたは RADIUS サーバにあるかにかかわらず「Stations List」内のクライアントに適用されます。
Stations List	これは、アクセスポイントを通じたネットワークへのアクセスを許可または拒否されるローカルなクライアントリストです。MAC アドレスをローカルな「Stations List」に追加するためには、下部にある欄に 48 ビットの MAC アドレスを入力します。 「Stations List」から MAC アドレスを削除するためには、48 ビットの MAC アドレスを選択して「Remove」ボタンをクリックします。リスト内のステーションは、前の欄で設定したフィルタの方法に基づいて許可または拒否されます。 **注意** VAP に対する MAC 認証タイプが Local に設定されている場合、アクセスポイントは、「Stations List」を使用してネットワークへのアクセスをクライアントに許可、または拒否することができます。VAP に対する MAC 認証タイプが RADIUS に設定されている場合、アクセスポイントは、このリストに設定されている MAC アドレスを無視して、RADIUS サーバに保存されているリストを使用します。MAC 認証は「VAP configuration」画面で設定されます。

注意 ローカル MAC 認証設定を実施後に「Apply」ボタンをクリックして変更を適用して設定を保存します。設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

RADIUS サーバに MAC 認証を設定する

MAC ベースのアクセス制御に RADIUS MAC 認証を使用する場合、RADIUS サーバにステーションリストを設定する必要があります。ステーションリストにはクライアントの MAC アドレスエントリが含まれます。リストの形式については以下の表で説明します。

RADIUS サーバ属性	説明	値
User-Name (1)	クライアントステーションの MAC アドレス。	有効なイーサネット MAC アドレス。
User-Password (2)	クライアントの MAC エントリ検索に使用する固定のグローバルパスワード。	NOPASSWORD

Load Balancing（ロードバランシングの設定）

ネットワーク利用率のしきい値を設定し、クライアントがアクセスポイントに接続または接続を解除する場合に無線ネットワークの速度と性能を維持することができます。ロードバランシング設定は両方の無線帯域に適用されます。

ロードバランシングを設定し、アクセスポイントの定義済みの稼動率によって起動されるように制限と動作を設定します。

Manage > Load Balancing の順にメニューをクリックし、以下の画面を表示します。

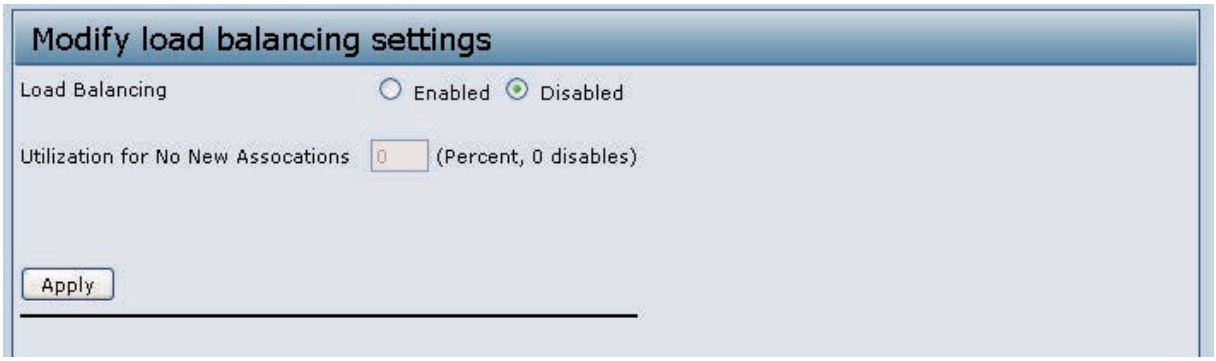


図 5-16　ロードバランシング設定の編集 画面

項目	説明
Load Balancing	ロードバランシングを有効または無効にします。 本アクセスポイントにおけるロードバランシング機能を有効「Enabled」または無効「Enabled」にします。有
Utilization for No New Associations	アクセスポイントが新しいクライアントの接続の受け入れを停止する前に、無線帯域で許可されるネットワーク帯域幅利用率（%）を提供します。 初期値は 0 で、これは、使用率に関わらず、すべての新しい接続を許可することを意味します。

注意 ロードバランシング設定を実施後に「Apply」ボタンをクリックして変更を適用し、設定を保存します。設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

Managed Access Point（管理アクセスポイントの設定）

本アクセスポイントは、2 つのモード（スタンドアロンモードまたは管理モード）のいずれかで動作します。スタンドアロンモードでは、本製品はネットワークで個々のアクセスポイントとして動作するため、Web マネージャ、CLI、または SNMP を使用することで管理します。管理モードでは、UAP は D-Link 統合アクセスシステムの一部となり、D-Link 統合スイッチを使用して管理を行います。アクセスポイントが本モードの場合、管理用 Web インタフェース、Telnet、SSH、および SNMP サービスはアクセスポイントで使用できなくなります。

本アクセスポイントでは、アクセスポイントを管理する 4 つの D-Link 統合スイッチの IP アドレスを設定することができます。アクセスポイントを管理するために、スイッチとアクセスポイントは相互に検出する必要があります。スイッチにはアクセスポイントを発見する複数の方法があります。スタンドアロンモードのアクセスポイントにスイッチの IP アドレスを登録することは、スイッチ -to- アクセスポイントの発見を有効にする 1 つの方法です。

モードの移行

30 秒ごとに、D-Link 統合スイッチは管理するアクセスポイントのすべてに keepalive メッセージを送信します。各アクセスポイントは、SSL TCP 接続に関する keepalive メッセージがないかどうかチェックします。アクセスポイントが keepalive メッセージを通じてスイッチとの通信を維持する限り、それは管理モードに残っています。

アクセスポイントが最後の keepalive メッセージから 45 秒以内にメッセージを受信しないと、アクセスポイントは、スイッチがエラーとなり、スイッチへの TCP 接続を終了したものと見なして、スタンドアロンモードに入ります。

アクセスポイントは、一度スタンドアロンモードに移行すると、損失なしでトラフィックの送信を続けます。アクセスポイントは、VLAN Forwarding モード（標準の non-tunneled モード）で設定された VAP において設定を使用します。

アクセスポイントがスタンドアロンモードの場合、Web インタフェースまたは CLI（Telnet または SSH 経由）を使用することで管理することができます。

アクセスポイントは、トンネル VAP を通じてアクセスポイントに接続するすべてのクライアントに対して、接続解除メッセージを送信し、トンネル VAP を無効にします。

「Managed AP Administrative Mode」が「Enabled」に設定されている間、アクセスポイントはディスカバリの手順を開始します。アクセスポイントが、以前に接続したスイッチと同じまたは違う無線スイッチと接続を確立しても、スイッチはアクセスポイントにコンフィグレーションを送信し、アクセスポイントは無線スイッチに現在接続するすべてのクライアントに関する情報を送信します。

スイッチから送信されたコンフィグレーションの適用後に、アクセスポイントの無線インタフェースは再起動します。無線インタフェースが動作状態となり、クライアントが再接続するまで、クライアントのトラフィックは簡単に中断されます。

管理アクセスポイントの設定

D-Link 統合スイッチの IP アドレスをアクセスポイントに追加します。

Manage > Managed Access Point の順にメニューをクリックし、以下の画面を表示します。

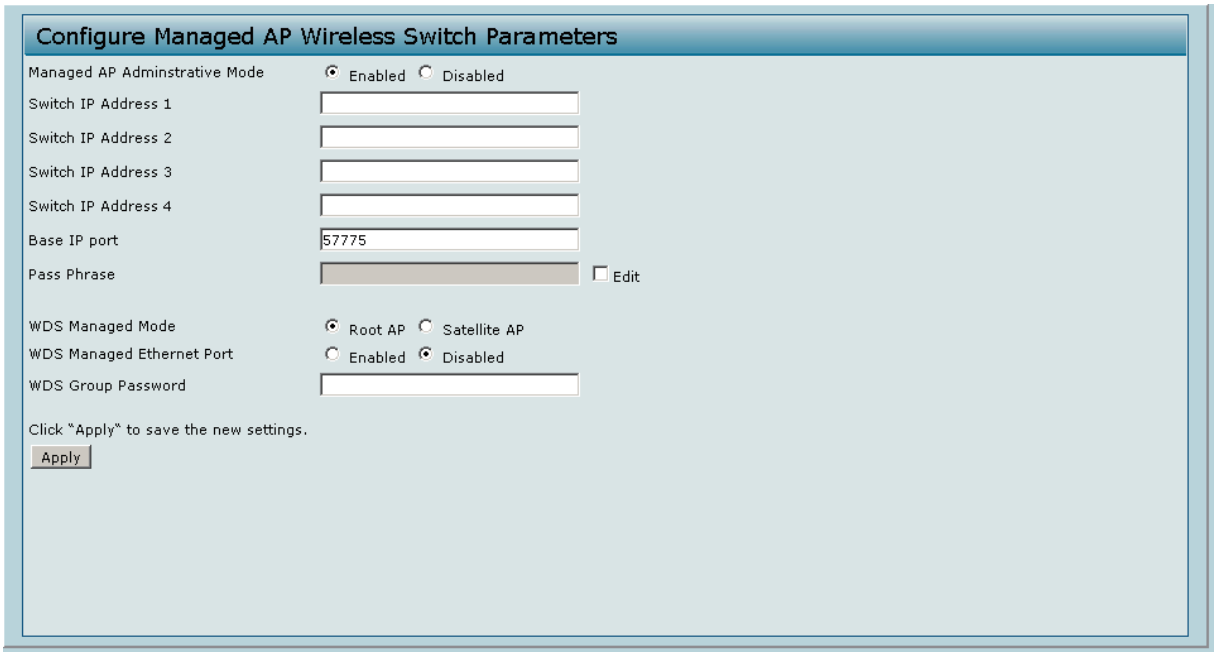


図 5-17　無線 AP 管理スイッチの設定 画面

以下の項目が表示されます。

項目	説明
Managed AP Administrative Mode	• Enabled - アクセスポイントとスイッチが相互にディスカバリを行うことを許可します。アクセスポイントが無線スイッチによる自身の認証に成功すると、Web 管理インタフェースにアクセスできなくなります。 • Disabled - アクセスポイントが無線スイッチとコンタクトをとることを防ぎます。
Switch IP address 1-4	アクセスポイントの管理に使用できる 4 台までの無線スイッチの IP アドレスを入力します。「.」（ドット）で区切った形式または DNS 名で IP アドレスを入力します。 DHCP サーバを使用することで設定済みのご使用のネットワークの無線スイッチのリストを参照することができます。 アクセスポイントは、最初に「Switch IP Address 1」とコンタクトを試みます。
Base IP Port	無線システムが IP トラフィックの送受信に使用する IP ポート番号の範囲を指定します。初期値では無線システムは「57775」から「57784」までの IP ポートを使用します。 基本 IP ポートを変更する場合、無線機能は自動的に無効となり、その後、再有効化されます。初期無線ポートはクラスタ設定関連コマンドのグローバルスイッチの一部として送信されないため、クラスタ内の全スイッチは個別に新しい IP 番号を設定される必要があります。 無線 IP ポート番号が初期値から変わった場合、AP 側も変更する必要があります。
Pass Phrase	「Edit」オプションを選択し、パスフレーズを入力して、アクセスポイントが無線スイッチで自身を認証することを許可します。パスフレーズは 8 ～ 63 文字です。 パスワードを削除するためには、「Edit」を選択し、既存のパスワードを削除した後に「Apply」ボタンをクリックします。スイッチには同じパスフレーズを設定する必要があります。
WDS Managed Mode	WDS グループ内にある時、「Root AP」または「Satellite AP」のどちらかになるように設定します。 • 「Root AP」— ブリッジまたはリピータとして、有線リンク経由のスイッチと通信します。 • 「Satellite AP」— WDS リンクの「Root AP」を経由してスイッチと通信をします。本モードでは「Satellite AP」によって「Root AP」との WDS リンクを構築、または検出することを有効にします。
WDS Managed Ethernet Port	AP が WDS グループの一部になる時、イーサネットポートが有効 / 無効になるか設定します。
WDS Group Password	WDS リンク構築のための「WPA2 Personal」認証のパスワードです。「Satellite AP」のみ本設定が必要になりまります。「Root AP」は管理される時にスイッチからパスワードを入手します。

注意 本画面で設定後、「Apply」ボタンをクリックして変更を適用して設定を保存します。設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

アクセスポイントが D-Link 統合スイッチによる認証に成功すると、Web マネージャを通じたアクセスポイントへの接続を喪失します。

Authentication（802.1X 認証の設定）

IEEE 802.1X のポートベースのネットワークアクセス制御を利用するネットワークでは、サプリカント（クライアント）は 802.1X オーセンティケータにアクセスが許可されるまで、ネットワークへアクセスすることができません。ネットワークで 802.1X 認証が使用されている場合は、アクセスポイントに 802.1X 認証情報を登録する必要があります。

Web インタフェースを使用して本製品の 802.1X サプリカントのユーザ名とパスワードを設定します。

Manage > Authentication の順にメニューをクリックし、以下の画面を表示します。

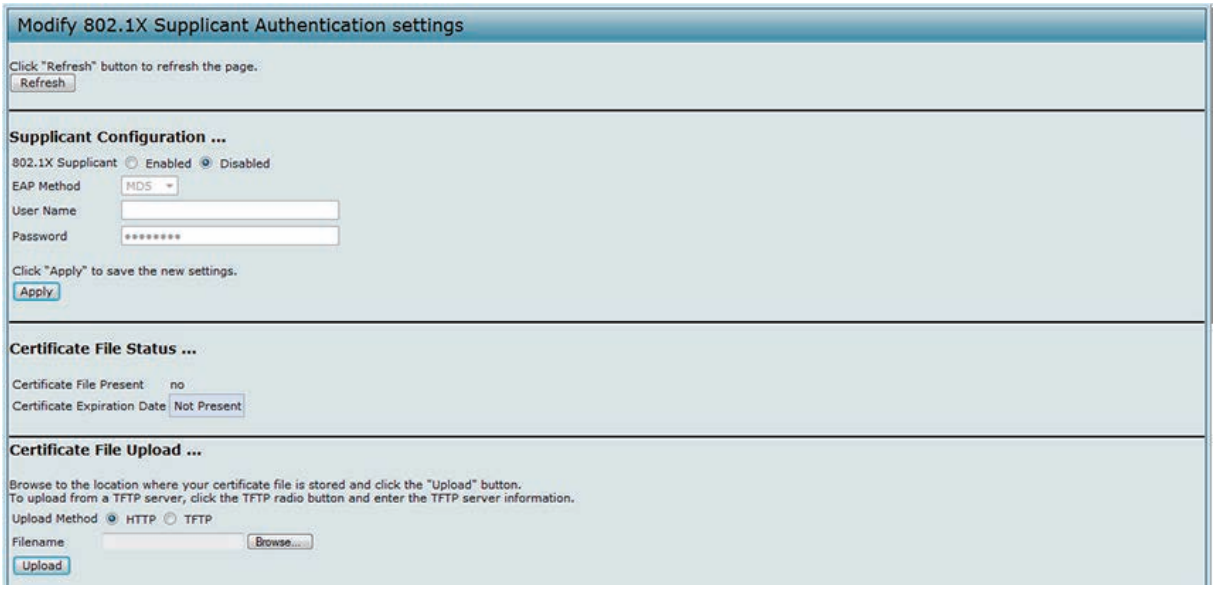

Modify 802.1X Supplicant Authentication settings
Click "Refresh" button to refresh the page.
Refresh
Supplicant Configuration ...
802.1X Supplicant Enabled Disabled
EAP Method MD5
User Name
Password
Click "Apply" to save the new settings.
Apply
Certificate File Status ...
Certificate File Present no
Certificate Expiration Date Not Present
Certificate File Upload ...
Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.
Upload Method HTTP TFTP
Filename
Browse...
Upload

図 5-18　IEEE 802.1X サプリカント認証設定の編集 画面

以下に示す項目を設定します。

項目	説明
802.1X Supplicant	• Enabled - 802.1X Supplicant の管理ステータスを有効にします。 • Disabled - 802.1X Supplicant の管理ステータスを無効にします。
EAP Method	次の EAP 方式から 1 つ AP と権限者の通信方法を選びます。 • MD5 • PEAP • TLS
Username	802.1X オーセンティケータからのリクエストに応じる場合にアクセスポイントが使用する MD5 ユーザ名を入力します。半角英数字 64 文字以内で指定します。キータイプは ASCII で、アルファベットの大文字、小文字、数字、および @# などの記号を含みます。
Password	802.1X オーセンティケータからのリクエストに応じる場合にアクセスポイントが使用する MD5 パスワードを入力します。半角英数字 64 文字以内で指定します。キータイプは ASCII で、アルファベットの大文字、小文字、数字、および @# などの記号を含みます。
Certificate File Status	認証が切れた時に認証ファイルの状態または認証が切れているかを表示します。
Certificate File Upload	認証ファイルをアップロードする方法を「HTTP」または「TFTP」から選択します。: •「HTTP」— 認証ファイルの保存場所を参照して「Upload」をクリックします。 •「TFTP」— 認証ファイルの保存場所と「TFTP」サーバの IP アドレス、ファイル名、パスを指定して「Upload」をクリックします。

注意　「Authentication」画面で設定後、「Apply」ボタンをクリックして変更を適用し、設定を保存します。設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

Management ACL（管理アクセスコントロールリストの作成）

Web ベースのアクセスポイント管理インタフェースにアクセスするために認可される最大 5 台の IPv4 ホストと 5 台の IPv6 ホストを示すアクセスコントロールリスト（ACL）を作成することができます。本機能を無効にすると、正しいアクセスポイントのユーザ名とパスワードを提供することで、どのネットワーククライアントからも管理インタフェースにアクセスできます。

アクセスコントロールリストを作成します。

Manage > Management ACL の順にメニューをクリックし、以下の画面を表示します。

図 5-19　管理アクセスコントロールパラメータの設定 画面

以下の項目を設定します。

項目	説明
Management ACL Mode	管理 ACL 機能を有効、または無効にします。管理 ACL モードを有効にする前に、少なくとも 1 つの IPv4 または IPv6 アドレスを設定する必要があります。有効にすると、指定した IP アドレスだけが管理インタフェースに対する Web、Telnet、SSH、および SNMP アクセスを持つことができます。
IP Address 1-5	アクセスポイントへの管理アクセスが許可される最大5つのIPv4アドレスを入力します。「.」（ドット）で区切った形式（例 192.168.10.10）を使用します。
IPv6 Address 1-5	アクセスポイントへの管理アクセスが許可される最大 5 つの IPv6 アドレスを入力します。標準の IPv6 アドレス形式（例 2001:0db8:1234::abcd）を使用します。

注意　設定後に「Apply」ボタンをクリックして変更を適用して設定を保存します。

第 6 章　Services（アクセスポイントサービスの設定）

ここでは本製品におけるサービスの設定方法について説明します。以下のサブセクションがあります。

設定項目	説明	参照ページ
Web Server（Web サーバの設定）	Web サーバの設定を行います。	85 ページ
SNMP（アクセスポイントの SNMP 設定）	SNMPv1 、SNMPv2c の設定を行います。	87 ページ
SSH（SSH ステータスの設定）	SSH アクセスを有効または無効にします。	89 ページ
Telnet（Telnet ステータスの設定）	Telnet アクセスを有効または無効にします。	89 ページ
QoS（QoS の設定）	QoS の設定を行います。	90 ページ
Email Alert（E メール警告）	E メールで送信されるアラートについて設定します。	92 ページ
Time Settings（NTP サーバの有効化）	NTP を使用してクロックタイムを同期させます。	94 ページ

本セクションの機能に対する設定画面は、メインメニューの「Manage」下におかれています。

Web Server（Web サーバの設定）

アクセスポイントは HTTP または Secure HTTP（HTTPS）を通じて管理できます。初期値では、HTTP と HTTPS の両方が有効です。個別にアクセスタイプを無効にすることができます。

Web サーバの設定を行います。

Services > Web Server の順にメニューをクリックし、以下の画面を表示します。

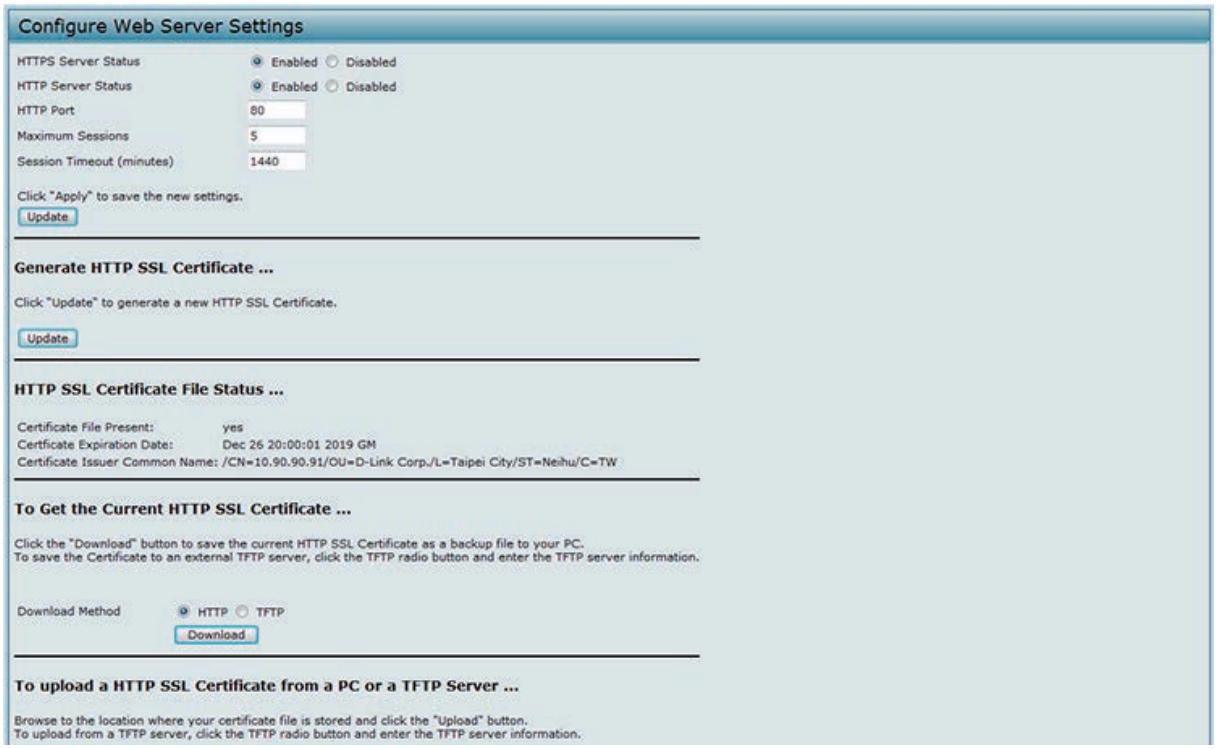

Configure Web Server Settings
HTTPS Server Status
Enabled
Disabled
HTTP Server Status
Enabled
Disabled
HTTP Port
80
Maximum Sessions
5
Session Timeout (minutes)
1440
Click "Apply" to save the new settings.
Update
Generate HTTP SSL Certificate ...
Click "Update" to generate a new HTTP SSL Certificate.
Update
HTTP SSL Certificate File Status ...
Certificate File Present: yes
Certficate Expiration Date: Dec 26 20:00:01 2019 GM
Certificate Issuer Common Name: /CN=10.90.90.91/OU=D-Link Corp./L=Taipei City/ST=Neihu/C=TW
To Get the Current HTTP SSL Certificate ...
Click the "Download" button to save the current HTTP SSL Certificate as a backup file to your PC.
To save the Certificate to an external TFTP server, click the TFTP radio button and enter the TFTP server information.
Download Method
HTTP
TFTP
Download
To upload a HTTP SSL Certificate from a PC or a TFTP Server ...
Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

図 6-1　Web サーバ設定 画面

項目	説明
HTTPS Server Status	Secure HTTP Server（HTTPS）を通じたアクセスを有効、または無効にします。
HTTP Server Status	HTTP を通じたアクセスを有効、または無効にします。本設定は HTTPS サーバステータス設定とは異なるものです。
HTTP Port	HTTP トラフィックにポート番号を指定します。初期値は 80 です。
Maximum Sessions	ユーザが AP の Web インタフェースにログオンする時、セッションが作成されます。セッションは不動作検知タイマが切れるか、ユーザがログオフするまで維持されます。 同時期に存在することが可能な Web セッション数を入力します（「HTTP」「HTTPs」を含む）。範囲は 1 から 10 です。もし Web セッションの最大数に達した場合、次にログオンしようとしたユーザにはセッション限界のエラーメッセージが表示され、ログオンできません。

項目	説明
Session Timeout	活動していないユーザが AP の Web インタフェースにログオンしていられる最大時間（分）を設定します。制限時間に達するとユーザは自動的にログオフされます。範囲は 1-1440 分です。
Generate HTTP SSL Certificate	Web サーバのセキュリティ用に新しい SSL 認証を設定するときに選択します。アクセスポイントが取得した IP アドレスが、統合 AP の IP アドレスと一致させる認証のために実施されます。SSL 認証を有効にするには Web サーバを再起動する必要があります。安全な接続は新しい認証がブラウザに承認されるまで、有効にはなりません。「Update」ボタンをクリックして新しい SSL 認証を有効化してください。
Generate SSL Certificate	本オプションを選択すると、セキュアな Web サーバのために新しい SSL 証明書を作成します。アクセスポイントが証明書の一般名が本製品の IP アドレスに一致することを保証する IP アドレスを一度持つとしたら、これが行われるべきです。新しい SSL 証明書を作成すると、セキュアな Web サーバは再起動します。セキュアな接続はブラウザで新しい証明書が受け付けられるまで動作しません。
HTTP SSL Certificate File Status	認証ファイルの状態と有効期限などの情報を表示します。
To Get the Current HTTP SSL Certificate	現在の「HTTP SSL」認証のコピーを TFTP サーバまたはローカルに保存します。 「HTTP」— 認証ファイルのバックアップコピーを保存する場所を指定し、「Download」をクリックします。 「TFTP」— 認証ファイル名、ファイルパス、認証ファイルコピーを保存する TFTP サーバの IP アドレスを指定して、「Download」をクリックします。
To upload a HTTP SSL Certificate from a PC or a TFTP Server	「HTTP」または「TFTP」を使用して、AP へ認証ファイルをアップロードします。 「HTTP」— 認証ファイルを保存する場所を指定して、「Upload」をクリックします。 「TFTP」— 認証ファイルを保存する TFTP サーバの場所、ファイル名、ファイルパスを指定して「Upload」をクリックします。

注意 「Apply」ボタンをクリックして変更を適用し、設定を保存します。アクセスポイントの管理インタフェースにアクセスするために現在使用しているプロトコルを無効にすると、現在の接続は終了し、有効にするまで、そのプロトコルを使用したアクセスポイントへのアクセスはできなくなります。

SNMP（アクセスポイントの SNMP 設定）

簡易ネットワーク管理プロトコル（SNMP:Simple Network Management Protocol）は、ネットワークデバイスの登録、保存、および共有情報のための標準プロトコルです。SNMP はネットワーク管理、トラブルシューティング、およびメンテナンスを容易にします。本アクセスポイントは、SNMP のバージョン 1（SNMP v1）、2c（SNMP v2c）、および 3（SNMP v3）を実装しています。明確に規定されない限り、本画面の全設定項目は、SNMPv1 と SNMPv2c だけに適用されます。

SNMP によって管理されるネットワークの重要な要素は、管理デバイス、SNMP エージェント、および管理システムです。エージェントは、Management Information Bases（MIBs）にデバイスに関するデータを保存し、要求に応じてこのデータを SNMP マネージャに返します。管理デバイスは、アクセスポイント、ルータ、スイッチ、ブリッジ、ハブ、サーバ、またはプリンタなどのネットワークノードです。

本製品は、HP OpenView などのネットワーク管理システムへのシームレスな統合のために SNMP が管理するデバイスとして機能することができます。

ここでは、SNMP エージェントの制御の開始または停止、コミュニティパスワードの設定、MIBs へのアクセス、および SNMP トラップの送信先の設定を行うことができます。

SNMPv3 メニューから、SNMPv3 ユーザとそれらのセキュリティレベルの管理、および SNMP MIBs に対するアクセス制御を定義することができます。SNMPv3 ビュー、グループ、ユーザ、およびターゲットの設定方法に関する情報については、「第 7 章　SNMPv3（SNMPv3 の設定）」（95 ページ）を参照してください。

SNMP を設定するためには、**Services > SNMP** の順にメニューをクリックして、以下の画面を表示します。

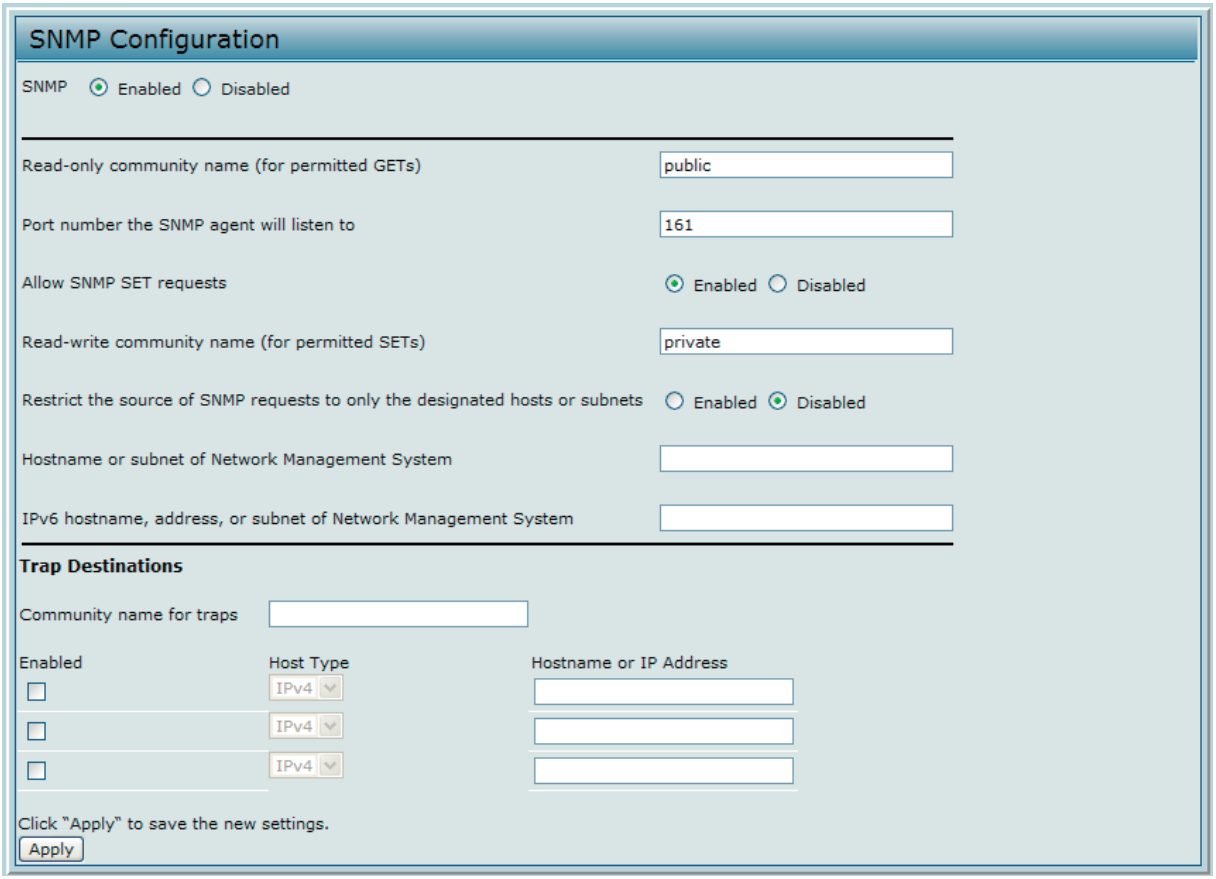


図 6-2　SNMP 設定の編集 画面

項目	説明
SNMP	ご使用のネットワークの SNMP の管理モードを指定します。初期値で SNMP は有効です。 • Enabled - SNMP を有効にします。 • Disabled - SNMP を無効にします。 モード変更後に、設定変更を保存するために「Apply」ボタンをクリックしする必要があります。 注意 SNMP を無効にすると、SNMP 画面の残りの項目すべてが無効にされます。これは、SNMPv1、SNMPv2c、および SNMPv3 に適用されるグローバルな SNMP パラメータです。
Read-only community name (for permitted GETs)	参照専用のコミュニティ名を入力します。 SNMPv2c で定義されるコミュニティ名は、SNMP エージェントにデータをリクエストできるネットワーク上のデバイスを制限するための簡単な認証メカニズムとして機能します。名称はパスワードのように機能し、送信側がパスワードを知っていると、そのリクエストは正しいものと見なされます。 コミュニティ名は半角英数字で指定されます。

項目	説明
Port number the SNMP agent will listen to	初期値では、SNMP エージェントはポート 161 からのリクエストだけをリッスンします。しかし、エージェントが別のポートでリクエストをリッスンできるように設定することができます。 SNMP エージェントにリクエストのリッスンを希望するポート番号を入力します。 **注意** これは、SNMPv1、SNMPv2c、および SNMPv3 に適用されるグローバルな SNMP パラメータです。
Allow SNMP SETs requests	アクセスポイントへの SNMP Set Request を許可するかどうかを選択します。SNMP Set Request を有効にすることは、ネットワーク上のデバイスがアクセスポイントの SNMP エージェントを経由して D-Link システム MIB に設定の変更を行うことができることを意味します。 • Enabled - SNMP Set Request を有効にします。 • Disabled - SNMP Set Request を無効にします。
Read-write community name (for permitted SETs)	SNMP Set Request を有効にすると、読み書き可能なコミュニティ名を設定できます。 コミュニティ名を設定することは、パスワードを設定することと同じです。このコミュニティ名で識別するデバイスからのリクエストだけが受け付けられます。 コミュニティ名は半角英数字で指定されます。
Restrict the source of SNMP requests to only the designated hosts or subnets	許可される SNMP リクエストの送信元を制限することができます。 • Enabled - 許可される SNMP リクエストの送信元を制限します。 • Disabled - SNMP リクエストを発行する送信元を許可します。
Hostname address or subnet of Network Management System	管理デバイスへのリクエストの取得および設定を実行するデバイスの IPv4 DNS ホスト名またはサブネットを指定します。コミュニティ名のように、これは SNMP 設定にセキュリティレベルを提供します。 SNMP エージェントはここで指定したホスト名またはサブネットからのリクエストだけを受け付けます。 サブネットを指定するために、address が IP アドレスで、mask_length がマスクビット数である「address/mask_length」形式で 1 つ以上のサブネットワークアドレスの範囲を入力します。 「address/mask」および「address/mask_length」の両方の形式をサポートしています。個々のホストは IP アドレスまたはホスト名などのために提供されます。例えば、1 つの範囲の「192.168.1.0/24」を入力すると、これはアドレス「192.168.1.0」と「255.255.255.0」のサブネットマスクでサブネットワークを指定します。 アドレス範囲は、指定された NMS のサブネットを指定するのに使用されます。この範囲内の IP アドレスを持つデバイスだけが、管理デバイスへのリクエストの取得および設定を実行するために許可されます。上記例では、192.168.1.1 ～ 192.168.1.254 にあるアドレスを持つマシンはデバイス上の SNMP コマンドを実行することができます。（サフィックス「.0」によってサブネットワーク範囲で特定されたアドレスは、サブネットワークアドレスのために常に予約され、範囲内の「.255」によって特定されたアドレスは、ブロードキャストアドレスのために常に予約されます。） 別の例として、10.10.1.128/25 デバイスの範囲を入力すると、10.10.1.129 ～ 10.10.1.254 にある IP アドレスを持つ IP アドレスは管理デバイスに SNMP リクエストを行うことができます。 本例では、「10.10.1.128」はネットワークアドレスで、「10.10.1.255」はブロードキャストアドレスです。126 個のアドレスを指定することができます。
IPv6 hostname, address, or subnet of Network Management System	管理デバイスへのリクエストの取得および設定を実行するデバイスの IPv6 DNS ホスト名またはサブネットを指定します。
Community name for traps	SNMP トラップに関連付けるグローバルなコミュニティの文字列を入力します。 デバイスから送信されたトラップは、コミュニティ名としてこの文字列を提供します。コミュニティ名は半角英数字で指定されます。特殊文字は許可されません。 • Enabled - 指定のトラップホストを有効にします。 • Host Type - トラップホストのタイプ（IPv4 または IPv6）を選択します。
Hostname or IP Address	トラップを SNMP に送信するコンピュータの DNS ホスト名を入力します。DNS ホスト名の例は、「snmptraps.foo.com」です。SNMP トラップは、SNMP エージェントからランダムに送信されるため、トラップが送信される正確な場所を指定する必要があります。最大 3 つの DNS ホスト名を追加することができます。適切なホスト名の横にある「Enabled」チェックボックスを選択します。

注意 SNMP 設定を実施後に「Apply」ボタンをクリックして変更を適用し、設定を保存します。設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

SSH（SSH ステータスの設定）

Secure Shell（SSH）は、リモートホストから本製品の CLI へのアクセスを提供するプログラムです。SSH は、保証されていないチャンネル上に強健な認証とセキュアな通信を供給するため、リモートアクセスには Telnet より安全性が高くなっています。「SSH」画面で、システムへの SSH アクセスを有効、または無効にすることができます。

Services > SSH の順にメニューをクリックし、以下の画面を表示します。

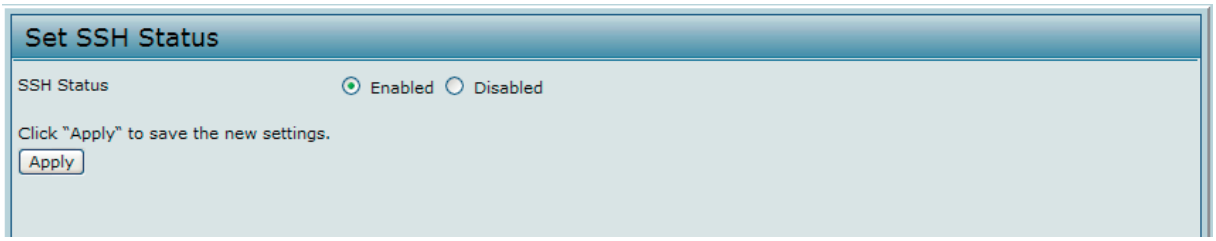


図 6-3　SSH ステータスの設定 画面

以下の項目を設定します。

項目	説明
SSH Status	アクセスポイントの CLI への SSH アクセスを有効、または無効にします。 • SSH を使用してアクセスポイントにリモートアクセスを許可するためには、「Enabled」をクリックします。 • SSH を使用してアクセスポイントにリモートアクセスを防ぐするためには、「Disabled」をクリックします。

Telnet（Telnet ステータスの設定）

Telnet は、リモートホストから本製品の CLI へのアクセスを提供するプログラムです。ここでは、システムへの Telnet アクセスを有効、または無効にします。

Telnet ステータスを設定するためには、**Services > Telnet** の順にメニューをクリックし、以下の画面を表示します。

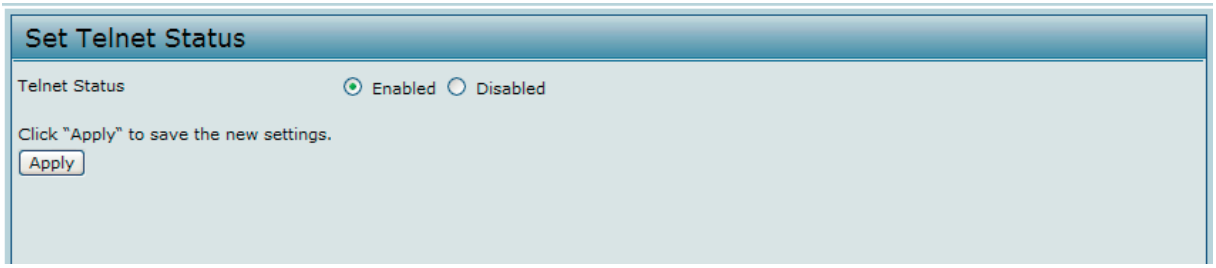


図 6-4　Telnet ステータスの設定 画面

以下の項目を設定します。

項目	説明
Telnet Status	アクセスポイントの CLI への Telnet アクセスを有効、または無効にします。 • Telnet を使用してアクセスポイントにリモートアクセスを許可するためには、「Enabled」をクリックします。 • Telnet を使用してアクセスポイントにリモートアクセスを防ぐするためには、「Disabled」をクリックします。

QoS（QoS の設定）

QoS（Quality of Service）機能は、複数のキューにパラメータを指定することで、本製品を通過する従来の IP データをはじめ VoIP（Voice over IP）や音声、映像、ストリーミングメディアなどの多くの無線トラフィックのスループットとパフォーマンスの向上を可能にします。

本製品に設定する QoS は、さまざまな種類の無線トラフィック用のキューにパラメータから構成され、伝送時の最大 / 最小待ち時間を（コンテンション画面により）効果的に指定することができます。ここで説明された設定は、データ伝送動作をアクセスポイントにだけ適用し、クライアントステーションには適用されません。

「AP EDCA（Enhanced Distributed Channel Access）Parameters」はアクセスポイントからクライアント向きのトラフィックフローに影響し、逆に「Station EDCA Parameters」は、クライアントからアクセスポイント向きのトラフィックフローに影響します。

アクセスポイントと「Station EDCA Parameters」の初期値は、WMM 仕様における Wi-Fi アライアンスによって示されているものです。通常の使用では、これらの値を変更する必要はありません。これらの値を変更、提供する QoS に影響します。

注意 DWL-6600AP と DWL8600AP では QoS 設定は両方の無線帯域に適用されますが、各帯域のトラフィックは個別にキューに独自に列におかれます。

QoS ステータスを設定するためには、**Services > QoS** の順にメニューをクリックし、以下の画面を表示します。

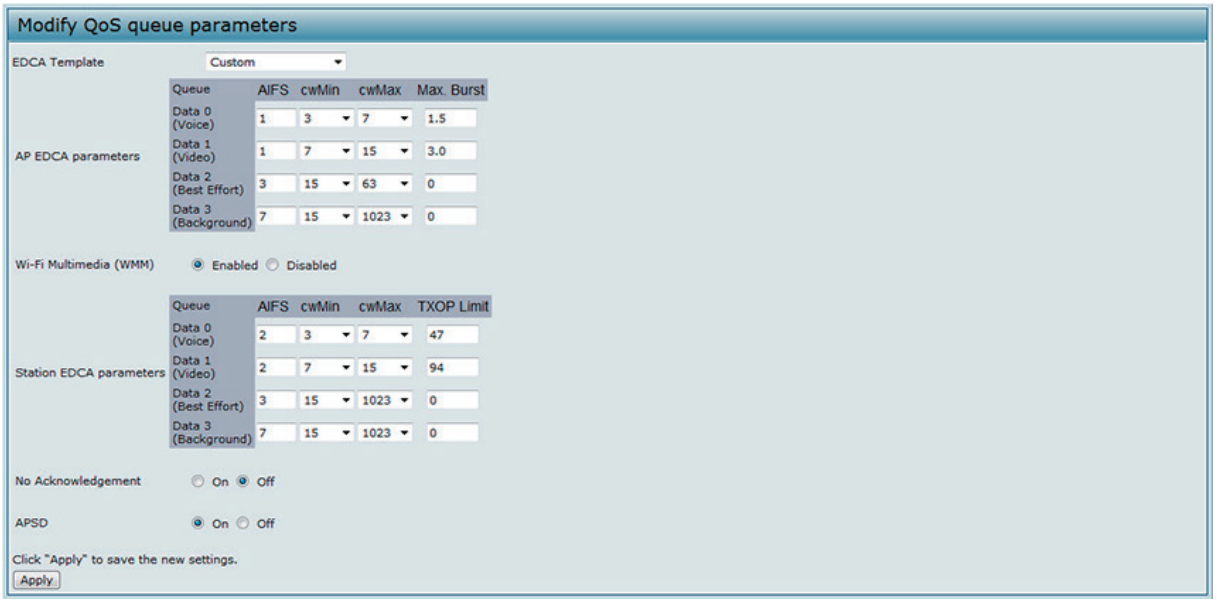

Modify QoS queue parameters
EDCA Template
Custom
AP EDCA parameters
Queue AIFS cwMin cwMax Max. Burst
Data 0 (Voice) 1 3 7 1.5
Data 1 (Video) 1 7 15 3.0
Data 2 (Best Effort) 3 15 63 0
Data 3 (Background) 7 15 1023 0
Wi-Fi Multimedia (WMM) Enabled Disabled
Station EDCA parameters
Queue AIFS cwMin cwMax TXOP Limit
Data 0 (Voice) 2 3 7 47
Data 1 (Video) 2 7 15 94
Data 2 (Best Effort) 3 15 1023 0
Data 3 (Background) 7 15 1023 0
No Acknowledgement On Off
APSD On Off
Click "Apply" to save the new settings.
Apply

図 6-5　QoS キューパラメータの設定 画面

以下の項目を設定します。

項目	説明
EDCA Template	Possible options are: Default, Optimized for Voice, and Custom.
AP EDCA parameters	
Queue	アクセスポイントからクライアントに送信する様々なデータタイプにキューを定義します。 • Data 0 (Voice) - 高優先度キュー、最小遅延。遅延に敏感な VoIP やストリーミングメディアなどのデータは自動的に本キューに送られます。 • Data 1 (Video) - 高優先度キュー、最小遅延。遅延に敏感なビデオデータは自動的に本キューに送られます。 • Data 2 (best effort) - 中優先度キュー、中スループット・中遅延。一般的な IP データは本キューに送られます。 • Data 3 (Background) - 最低優先度キュー、高スループット。高いスループットを要する大容量データや、遅延に敏感ではないデータは本キューに送られます（例 : FTP データなど）。
AIFS	AIFS（Arbitration Inter-Frame Spacing）では、データフレーム間の待ち時間を指定します。待ち時間はスロットで測定されます。1 から 255 の間の値を指定します。単位はミリ秒です。
cwMin	この値は、伝送リトライの " 初回ランダムバックオフ待ち時間 " を定義するアルゴリズムに使用します。 この値は、" 初回ランダムバックオフ待ち時間 " の範囲の上限（ミリ秒）として「Minimum Contention Window」画面で指定します。 1 番目のランダム（任意）番号は、0 から本欄で指定する値の中から生成されます。 データフレームが送信される前に、1 番目のランダムバックオフ待ち時間が失効すると、リトライカウンタは 1 増加し、ランダムバックオフ値は 2 倍の値になります。このランダムバックオフ値が、次の欄の cwMax で定義する値に到達するまで、失効に伴って値を倍にしていきます。 cwMin に対する有効な値は、1,3,7,15,31,63,127,255,511, または 1023 です。cwMin 値には cwMax で定義する値より小さい値を指定してください。

項目	説明
cwMax	この値は、ランダムバックオフ値の上限で、「Maximum Contention Window」画面で指定します。ランダムバックオフ値は、データフレームが送信されるか、本欄で指定した値に到達するまで、倍掛けされていきます。単位はミリ秒です。 ランダムバックオフ値が、本欄で指定した値に到達すると、リトライは " リトライ許可最大回数 " に到達するまで継続されます。 cwMax に対する有効な値は、1,3,7,15,31,63,127,255,511, または 1023 です。cwMax 値には cwMin で定義する値より大きい値を指定してください。
Max. Burst	これは、AP EDCA パラメータで、アクセスポイントからクライアントステーションへのトラフィックフローに対してのみ適用されます。 本値は無線ネットワークでのパケットバーストに認められる最大バースト長です。パケットバーストとはヘッダ情報なしで送信できる複数のフレームの集まりです。オーバヘッドを少なくすることにより、高スループットと高パフォーマンスを実現できます。 最大バースト長に有効な値は、0.0 から 999 です。
Wi-Fi Multimedia (WMM)	
Wi-Fi MultiMedia (WMM)	WMM（Wi-Fi Multimedia）機能は、初期値で有効です。WMM が有効であると、QoS 優先制御や無線メディアアクセスの調整も有効になります。また、本アクセスポイントの QoS 設定は上りと下り両方のトラフィック（クライアントからアクセスポイント（Station EDCA パラメータ）、およびアクセスポイントからクライアント（AP EDCA パラメータ））に対して有効になります。 WMM を無効に設定すると、上りのトラフィック（クライアントからアクセスポイント）における「Station EDCA パラメータ」の QoS 制御は無効になります。 WMM が無効状態の時でも、" アクセスポイントからクライアントへの下り方向（AP EDCA パラメータ）" のいくつかのパラメータは設定可能です。 WMM 機能を無効にするためには「Disabled」を、有効にするためには「Enabled」を選択してください。
Station EDCA parameters	
Queue	ステーションからアクセスポイントに送信する様々なデータタイプにキューを定義します。 • Data 0 (Voice) - 最高優先度キュー、最小遅延。遅延に敏感な VoIP やストリーミングメディアなどのデータは自動的に本キューに送られます。 • Data 1 (Video) - 最高優先度キュー、最小遅延。遅延に敏感なビデオデータは自動的に本キューに送られます。 • Data 2 (best effort) - 中優先度キュー、中スループット・中遅延。一般的な IP データは本キューに送られます。 • Data 3 (Background) - 最低優先度キュー、高スループット。高いスループットを要する大容量データや、遅延に敏感ではないデータは本キューに送られます（例 : FTP データなど）。
AIFS (Inter-Frame Space)	AIFS（Arbitration Inter-Frame Spacing）では、データフレーム間の待ち時間を指定します。待ち時間はスロットで測定されます。1 から 255 の間の値を指定します。単位はミリ秒です。
cwMin	本パラメータは、UAP のリソース用のコンテンション期間のデータ転送のために " 初回ランダムバックオフ待ち時間 " を定義するアルゴリズムに使用されます。これは値は、" 初回ランダムバックオフ待ち時間 " の範囲の上限として指定します。単位はミリ秒です。 1 番目のランダム（任意）番号は、0 から本欄で指定する値の中から生成されます。データフレームが送信される前に、1 番目のランダムバックオフ待ち時間が失効すると、リトライカウンタは 1 増加し、ランダムバックオフ値は 2 倍の値になります。このランダムバックオフ値が、次の欄の cwMax で定義する値に到達するまで、失効に伴って値を倍にしていきます。
cwMax	本パラメータは、ランダムバックオフ値の上限です。ランダムバックオフ値は、データフレームが送信されるか、本欄で指定した値に到達するまで、倍掛けされていきます。単位はミリ秒です。 ランダムバックオフ値が、本欄で指定した値に到達すると、リトライは " リトライ許可最大回数 " に到達するまで継続されます。
TXOP Limit	これは、Station EDCA パラメータで、クライアントステーションからアクセスポイントへのトラフィックフローに対してのみ適用されます。TXOP（Transmission Opportunity: 送信権）は、WME クライアントステーションが本製品に向かって無線メディアで送信を始める権利を持つ場合に発生する間隔です。最大値は 65535 です。
他の QoS 設定	
No Acknowledgement	「On」を選択して、アクセスポイントがサービスクラス値として QosNoAck を持つフレームを承認するべきでないことを指定します。
APSD	「On」を選択して、電源管理方法である自動省電力機能（APSD）を有効にします。APSD は、VoIP 電話がアクセスポイントを通じてネットワークにアクセスする場合にお勧めします。

注意 QoS 設定を実施後に「Apply」ボタンをクリックして変更を適用し、設定を保存します。設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

Email Alert（E メール警告）

「Email Alert」機能は幾つかのレベル分けされたイベントによって AP が自動的に E メールを送信する機能です。「Email Alert」機能の使用には、メールサーバの設定、警告発信トリガレベルの設定、3 つまでのメールアカウント設定（緊急時 / 非緊急時）などを設定する必要があります。

注意 AP が管理モードの場合本機能は使用できません。

Services > Email Alerts の順にメニューをクリックし、以下の画面を表示します。

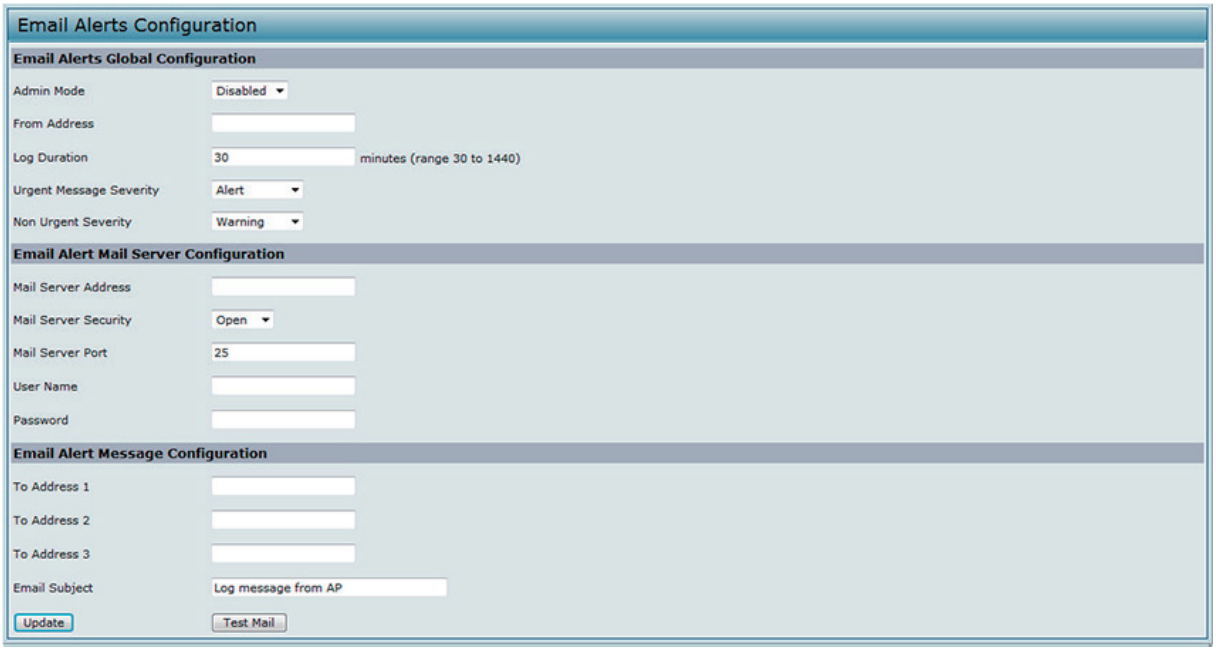


図 6-6　Email Alerts 画面

ネットワークタイムプロトコル（NTP）サーバを使用するようにアクセスポイントを設定するためには、最初に NTP の使用を有効にし、次に使用する NTP サーバを指定します。

項目	説明
Email Alert Global Configuration	
Admin Mode	「Email Alert」機能をグローバルに有効にします。初期値は無効です。
From Address	AP から送信される E メールの送信メールアドレスを設定します。255 字（英数半角）までのアドレスを設定可能です。初期値ではアドレスは登録されていません。
Log Duration	SMTP サーバに送信される非緊急メールの頻度を記録するログ期間を設定します。範囲は 30 ～ 1440 分です。初期値は 30 分です。
Urgent Message Severity	「urgent/（緊急）」と認識されるログのレベルを選択します。本カテゴリ内のメッセージはすぐに送信されます。 「Emergency」はシステムが動作していない状態を示します。最高位の警告です。 「Alert」はすぐに対処するべき事項に関する警告です。 「Critical」危険な状態であることを示しています。 「Error」はエラーが発生してる状態であることを示します。 「Warning」は警告状態であることを示します。 「Notice」は通常の状態ですが、何か示唆する状況にあります。 「Info」はお知らせがあります。 「Debug」はデバッグレベルのメッセージです。
Non Urgent Severity	それほど緊急ではない（Not Urgent）の状態を示すログメッセージのレベルです。 本カテゴリのメッセージは「Log Duration」項目で設定されたインターバル時間にダイジェストフォームで収集 / 送信されます。本項目で選択されたセキュリティレベルとそれ以上のレベルは非緊急 /Non Urgent として認識されます。 これよりも低いセキュリティレベルで設定されたメッセージは E メールで送信されることはありません。 セキュリティレベルについては「Urgent Message」を参照してください。
Email Alert Mail Server Configuration	
Mail Server Address	ネットワーク上の SMTP サーバの IP アドレスまたはホスト名を指定します。
Mail Server Security	メールサーバのための認証として、「SMTP over SSL」(TLSv1) または「セキュリティ無し」(Open) にするか設定します。初期値は Open です。
Mail Server Port	SMTP の TCP ポート番号を設定します。範囲は 0 から 65535 までの有効なポート番号です。初期値は 25、これは通常の SMTP ポートの番号です。
Username	メールサーバの認証が必要な場合のユーザ名を指定します。ユーザ名は 64 バイト文字です。初期値は「admin」です。

項目	説明
Password	前項で設定したユーザ名に対応するパスワードを設定します。
Email Alert Message Configuration	
To Address 1	警告メールが送信される最初のアドレスを設定します。有効なアドレスに限ります。初期値ではアドレスは設定されていません。
To Address 2	オプションとして警告メールが送信される 2 番目のメールを設定します。有効なアドレスに限ります。初期値ではアドレスは設定されていません。
To Address 3	オプションとして警告メールが送信される 3 番目のメールを設定します。有効なアドレスに限ります。初期値ではアドレスは設定されていません。
Email Subject	警告メールの件名部分を設定します。255 文字の英数字が使用可能です。初期値は「Log message from AP」です。

注意 「Email Alert」の設定後、「Apply」をクリックして設定を有効にしてください。

注意 設定したメールサーバの状態を確かめるには「Test Mail」をクリックしてテストメールを送信し、メールサーバの状態を確かめることが可能です。

AP からネットワーク管理者に送られるメール警告は以下のようになります。

From: AP-192.168.2.10@mailserver.com
Sent: Wednesday, July 08, 2011 11:16 AM
To: administrator@mailserver.com
Subject: log message from AP

TIME	Priority	Process Id	Message
Jul 8 03:48:25	info	login[1457]	root login on 'ttyp0'
Jul 8 03:48:26	info	mini_http-ssl[1175]	Max concurrent connections of 20 reached

Time Settings（NTP サーバの有効化）

NTP（Network Time Protocol ）は、ご使用のネットワークのコンピュータクロックタイムを同期させるインターネット標準プロトコルです。
NTP サーバは協定世界時（また、グリニッジ標準時として知られている協定世界時）をそれらのクライアントシステムに送信します。NTP は定期的に時間の要求をサーバに送信し、返されたタイムスタンプを使用してクロックを調整します。タイムスタンプは、ログメッセージ内の各イベントの日時を示すのに使用されます。

NTP に関する詳しい情報については http://www.ntp.org を参照してください。

アクセスポイントが使用する NTP サーバのアドレスを設定します。

Services > Timeの順にメニューをクリックし、以下の画面を表示します。本画面は、メインメニューの**Tools > SNTP**メニューからもアクセス可能です。

図 6-7　アクセスポイントの時間取得方法の設定 画面

ネットワークタイムプロトコル（NTP）サーバを使用するようにアクセスポイントを設定するためには、最初に NTP の使用を有効にし、次に使用する NTP サーバを指定します。

項目	説明
Set System Time	NTP は、アクセスポイントにネットワークのサーバから時間を取得して保持する方法を提供します。NTP サーバを使用すると、アクセスポイントにログメッセージとセッション情報に正しい時刻を提供することができます。 ネットワークタイムプロトコル（NTP）サーバの使用を有効または無効にします。 • Enabled - アクセスポイントに NTP サーバへのポーリングを許可します。 • Disabled - アクセスポイントの NTP サーバへのポーリングをブロックします。
NTP Server	NTP を有効にした場合に、使用する NTP サーバを指定します。 NTP サーバのホスト名または IP アドレスを指定します。IP アドレスの使用は、これらが容易に変更されてしまうことから推奨されません。
System Date (Manual configuration)	月、日、年を指定します。（手動）
System Time (Manual configuration)	現在時刻を指定します。システムは 24 時間計を使用します。午後 6 時は「18:00」と表示されます。
Time Zone	メニューからタイムゾーンを選択します。初期値は「USA」(Pacific) になっています。
Adjust Time for Daylight Savings	「Daylight Savings Time」(DST)（サマータイム）システムの使用有無を選択します。 本項目を選択すると設定が可能になります。
DST Start (24 HR)	「Daylight Savings Time」(DST)（サマータイム）の開始日時を設定します。
DST End (24 HR)	「Daylight Savings Time」(DST)（サマータイム）の終了日時を設定します。
DST Offset (minutes)	「Daylight Savings Time」(DST)（サマータイム）のオフセットを設定します。初期値は 60 分です。

注意　時間設定を実施後にて保存します。設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

第 7 章　SNMPv3（SNMPv3 の設定）

本セクションでは、SNMPv3 に関する概要を提供し、「SNMPv3」メニューで可能な機能について記述しています。本セクションには以下のサブセクションがあります。

設定項目	説明	参照ページ
SNMPv3 Views（SNMPV3 ビューの設定）	SNMPv3 ユーザがアクセスできる OID 範囲を制御するために MIB ビューを作成します。	95 ページ
SNMPv3 Groups（SNMPv3 グループの設定）	異なる許可とアクセス権を持つ SNMPv3 グループを設定します。	96 ページ
SNMPv3 Users（SNMPv3 ユーザの設定）	各ユーザにセキュリティレベルを設定します。	97 ページ
SNMPv3 Targets（SNMPv3 ターゲットの設定）	SNMPv3 ターゲットの設定を行います。	98 ページ

SNMPv3 Views（SNMPv3 ビューの設定）

MIB ビューは、ビューサブツリーのセットまたはビューサブツリーファミリーの組み合わせで、各ビューツリーが管理対象のオブジェクト名ツリーの内側のサブツリーです。SNMPv3 ユーザがアクセスできる OID 範囲を制御するために MIB ビューを作成できます。

「All」と呼ばれる MIB ビューは、システムに初期値で作成されています。このビューはシステムによってサポートされるすべての管理オブジェクトを含んでいます。

注意 Excluded ビューサブツリーを作成する場合、Excluded サブツリーの外側のサブツリーを含めることを許可するためには、同じビュー名を持つ対応する Included エントリを作成します。例えば、サブツリー 1.3.6.1.4 を除くビューを作成するためには、OID 1.3.6.1.4 を持つ Excluded エントリを作成します。その後、同じビュー名を持つ OID.1 の Included エントリを作成します。

SNMPv3 > SNMPv3 Views の順にメニューをクリックし、以下の画面を表示します。

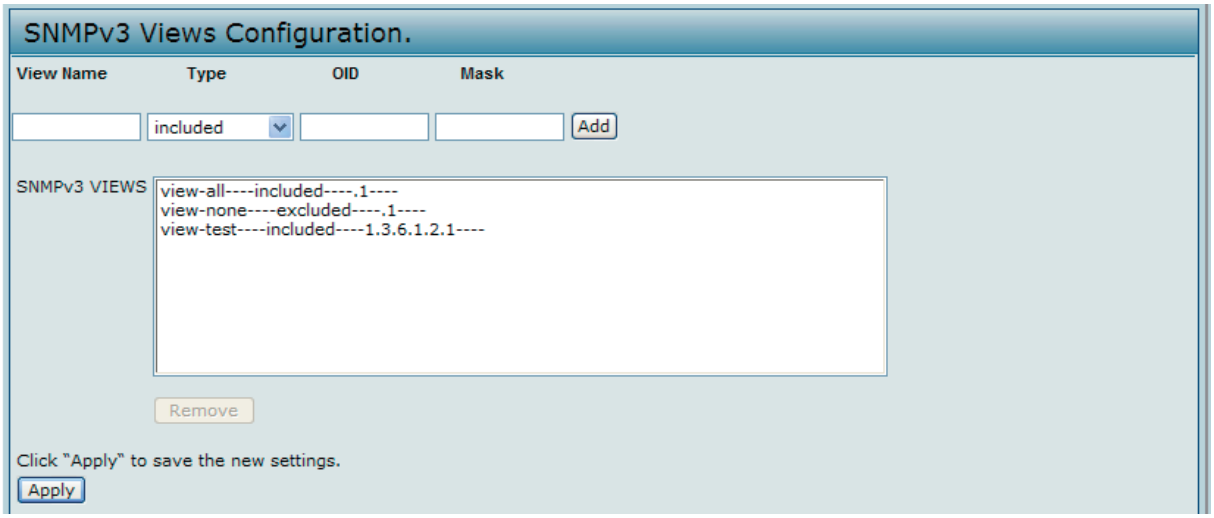


図 7-1　SNMPv3 ビューの設定 画面

「View Name」、「Type」、「OID」、「Mask」を指定後、「Add」ボタンをクリックして「SNMPv3 VIEWS」テーブルにエントリを追加します。

以下の表は、「SNMPv3 Views」画面で設定する各項目について説明しています。

項目	説明
View Name	MIB ビューを識別する名称を入力します。半角英数字 32 文字以内。
Type	MIB ビューからビューサブツリーまたはサブツリーのファミリーを「included」（含める）か、「excluded」（除外する）かを指定します。
OID	ビューに含める、またはビューから除くサブツリーの OID 文字列を入力します。例えば、システムサブツリーは、OID 文字列 1.3.6.1.2.1.1 で指定されます。
Mask	OID マスクの長さは 47 文字です。OID マスクのフォーマットは、「xx.xx.xx...」であり、長さは 16 オクテットです。各オクテットは「.」（ピリオド）または「:」（コロン）のどちらかによって区切られた 2 桁の 16 進数です。本欄は 16 進数だけを受け付けます。例えば、OID マスク「FA.8」は「11111010.10000000」です。 ファミリーマスクは、ビューサブツリーのファミリーを定義するのに使用されます。ファミリーマスクは、関連するファミリー OID の文字列のどのサブ識別子がファミリーの定義に重要であるかを示します。ビューサブツリーのファミリーにより、より効率的な方法でテーブル内の 1 列に対してアクセス制御を許可します。省略することができます。
SNMPv3 VIEWS	本製品における MIB ビューを示します。ビューを削除するためには、削除するビューを選択し、「Remove」ボタンをクリックします。

エントリの削除

削除するビューを選択し、「Remove」ボタンをクリックします。

注意 SNMPv3 ビュー設定を実施後に「Apply」ボタンをクリックして変更を適用し、設定を保存します。

SNMPv3 Groups（SNMPv3 グループの設定）

SNMPv3 グループにより、異なる許可とアクセス権のグループにユーザをまとめることができます。

初期値では、UAP には 3 つのグループがあります。

- RO - 認証とデータの暗号化のない読み取り専用グループ。本グループには何のセキュリティも提供されません。初期値では、本グループのユーザは、ユーザが編集できるすべての MIB ビューの初期値を参照することができます。
- RWAuth - 認証を使用するが、データ暗号化のない read/write（読み書き）グループ。本グループにおけるユーザは、認証には MD5 キー / パスワードを使用するメッセージを SNMP に送信しますが、暗号化のための DES キー / パスワードは送信しません。初期値では、本グループのユーザは、ユーザが編集できるすべての MIB ビューの初期値を読み書きすることができます。
- RWPriv - 認証とデータ暗号化を使用する read/write（読み書き）グループ。本グループにおけるユーザは、認証には MD5 キー / パスワード、および暗号化には DES キー / パスワードを使用します。MD5 と DES キー / パスワードの両方を定義する必要があります。初期値では、本グループのユーザは、ユーザが編集できるすべての MIB ビューの初期値を読み書きすることができます。

RWPriv、RWAuth、および RO グループは初期値で定義されています。

追加グループを定義するためには、**SNMPv3 > SNMPv3 Groups** の順にメニューをクリックし、以下の画面を表示します。

図 7-2　SNMPv3 グループの設定 画面

各項目を入力し、「Add」ボタンをクリックして「SNMPv3 GROUPS」テーブルにエントリを追加します。

以下の項目が表示されます。

項目	説明
Name	グループを識別する名称を入力します。初期グループ名は、RWPriv、RWAuth、および RO です。グループ名には半角英数字 32 文字以内で指定します。
Security Level	このグループに対して以下のセキュリティレベルの 1 つ選択します。 • noAuthentication-noPrivacy - 認証とデータ暗号化の両方がありません。（セキュリティなし） • Authentication-noPrivacy - 認証はありますが、データ暗号化はありません。このセキュリティレベルを使用すると、ユーザは、認証には MD5 キー / パスワードを使用するメッセージを SNMP に送信しますが、暗号化のための DES キー / パスワードは送信しません。 • Authentication-Privacy - 認証とデータ暗号化。このセキュリティレベルを使用すると、ユーザは、認証には MD5 キー / パスワード、および暗号化には DES キー / パスワードを送信します。 認証、暗号化、およびその両方を必要とするグループのために、「SNMPv3 Users」画面で MD5 と DES キー / パスワードを定義する必要があります。
Write Views	グループに管理オブジェクト（MIBs）に対するアクセス（書き込み）を選択します。 • view-all - グループは、MIBs を作成、変更、および削除できます。 • view-none - グループは、MIBs を作成、変更、または削除できません。
Read Views	グループに管理オブジェクト（MIBs）に対するアクセス（読み出し）を選択します。 • view-all - グループは、すべての MIBs の参照および読み出しができます。 • view-none - グループは MIBs の参照も読み出しもできません。
SNMPv3 GROUPS	本欄は、デフォルトグループとアクセスポイントで定義したグループを示しています。グループを削除するためには、グループを選択し、「Remove」ボタンをクリックします。

SNMPv3 ビュー設定を実施後に「Apply」ボタンをクリックして変更を適用して設定を保存します。

注意　SNMPv3 グループ設定を実施後に「Apply」ボタンをクリックして変更を適用し、設定を保存します。

SNMPv3 Users（SNMPv3 ユーザの設定）

複数ユーザを定義して、各ユーザに希望するセキュリティレベルの割り当て、およびセキュリティキーの設定を行うことができます。認証には MD5 タイプ、暗号化には DES タイプだけがサポートされています。本製品には SNMPv3 ユーザの初期値はありません。

SNMPv3 > SNMPv3 Users の順にメニューをクリックし、以下の画面を表示します。

図 7-3　SNMPv3 ユーザの設定 画面

各項目を入力し、「Add」ボタンをクリックして「SNMPv3 USERS」テーブルにエントリを追加します。

以下の表は、SNMPv3 ユーザを設定する項目について説明しています。

項目	説明
Name	SNMPv3 ユーザを識別する名称を入力します。ユーザ名は半角英数字 32 文字以内で指定します。
Group	ユーザをグループにマップします。初期グループは、RWPriv、RWAuth、および RO です。「SNMPv3 Groups」画面で追加グループを定義することができます。
Authentication Type	ユーザからの SNMP リクエストに使用する認証タイプを選択します。 • MD5 - ユーザからの SNMPv3 リクエストに MD5 認証を必要とします。 • None - ユーザからの SNMPv3 リクエストは何の認証も必要としません。
Authentication Key	認証タイプとして MD5 を指定した場合、パスワードを入力して、ユーザが送信したリクエストの認証を行うために SNMP エージェントを有効にします。パスフレーズは 8 - 32 文字とします。
Encryption Type	ユーザからの SNMP リクエストに使用する暗号化のタイプを選択します。 • DES - ユーザからの SNMPv3 リクエストに DES 暗号化を使用します。 • None - ユーザからの SNMPv3 リクエストは何の暗号化も必要としません。
Encryption Key	暗号化タイプとして DES を指定した場合、キーを入力して、SNMP 要求を暗号化します。パスフレーズは 8 - 32 文字です。
SNMPv3 USERS	本欄は、アクセスポイントに定義したユーザを示しています。ユーザを削除するためには、ユーザを選択し、「Remove」ボタンをクリックします。

注意　SNMPv3 ユーザ設定を実施後に「Apply」ボタンをクリックして変更を適用し、設定を保存します。

SNMPv3 Targets（SNMPv3 ターゲットの設定）

SNMPv3 ターゲットは、SNMP マネージャにトラップメッセージを送信します。各ターゲットは、ターゲット名で識別され、ターゲット IP アドレス、UDP ポート、および SNMP ユーザ名に関連付けられます。

SNMPv3 > SNMPv3 Targets の順にメニューをクリックし、以下の画面を表示します。

図 7-4　SNMPv3 ターゲットの設定 画面

各項目を入力し、「Add」ボタンをクリックして「SNMPv3 TARGETS」テーブルにエントリを追加します。

以下の項目が表示されます。

項目	説明
IPv4/IPv6 Address	リモートの SNMP マネージャの IP アドレスを入力して、トラップメッセージを受信するターゲットホストを指定します。
Port	SNMP ターゲットを送信するために使用する UDP ポートを入力します。
Users	ターゲットに割り当てる SNMP ユーザ名を入力します。SNMP ユーザの設定方法については「SNMPv3 Users（SNMPv3 ユーザの設定）」（97 ページ）を参照してください。
SNMPv3 TARGETS	本製品における SNMPv3 ターゲットを示します。ターゲットを削除するためには、削除するターゲットを選択し、「Remove」ボタンをクリックします。

注意　SNMPv3 ターゲット設定を実施後に「Apply」ボタンをクリックして変更を適用し、設定を保存します。

第 8 章　Maintenance（メンテナンス）

ここでは本製品のメンテナンス方法について説明します。本製品の管理者用ユーザインタフェースから以下のメンテナンスを行うことができます。

設定項目	説明	参照ページ
Configuration Save（コンフィグレーションの保存）	現在のコンフィグレーションファイルを保存します。	99 ページ
Configuration Restore（コンフィグレーションのリストア）	保存したコンフィグレーションをリストアします。	101 ページ
Maintenance（リセットと再起動）	本製品の工場出荷時設定へのリセット、および再起動を行います。	103 ページ
Upgrade（ファームウェアの更新）	ファームウェアを最新バージョンに更新します。	104 ページ
Packet Capture（Packet Capture の設定）	パケットキャプチャの設定をします。	106 ページ

Configuration Save（コンフィグレーションの保存）

本製品のコンフィグレーションファイルは XML フォーマットで作成され、設定に関する情報をすべて含んでいます。コンフィグレーションファイルは、管理ステーションにダウンロードすることができ、内容の編集を手動で行い、バックアップとして保存することができます。

本製品のファイル転送には、HTTP または TFTP を使用することができます。コンフィグレーションファイルを管理ステーションにダウンロードした後、XML フォーマットのコンフィグレーションファイルの編集を手動で行うことが可能です。編集したコンフィグレーションファイルは、本製品にアップロードして新たな設定を適用させることもできます。

Maintenance > Configuration Save の順にメニューをクリックします。ツールメニューの **Configuration > Configuration Save** からもアクセスすることもできます。

現在のコンフィグレーションのコピーを作成し、バックアップファイルに保存します。

TFTP を使用して行う手順

1. 「Download Method」の「TFTP」をチェックします。

図 8-1　アクセスポイントのコンフィグレーションの管理 画面 - 保存

2. 「Configuration File」に拡張子「.xml」のファイル名とファイルを保存するディレクトリへのパスを含むバックアップファイル名を入力します。

3. 「Server IP」に TFTP サーバの IP アドレスを入力します。

4. 「Download」ボタンをクリックしてコンフィグレーションファイルを保存します。

HTTP を使用して行う手順

1. 「Download Method」の「HTTP」をチェックします。

2. 「Download」ボタンをクリックすると、以下のダイアログが表示されます。

図 8-2　ダウンロードの確認ダイアログ

3. 「OK」ボタンをクリックすると、「ファイルのダウンロード」ダイアログが表示されます。

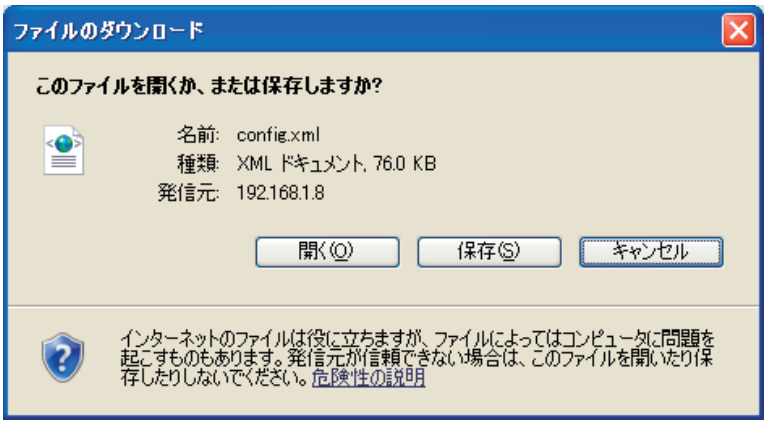


図 8-3 「ファイルのダウンロード」ダイアログ

4. 「保存」ボタンをクリックすると、「名前を付けて保存」のダイアログが表示されます。

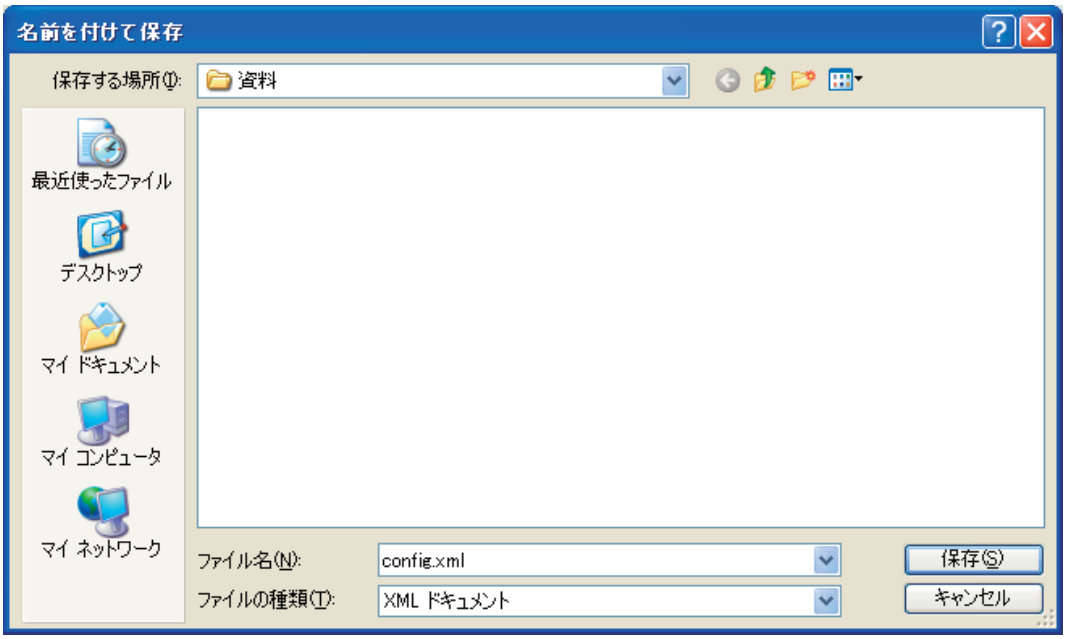


図 8-4 「名前を付けて保存」ダイアログ

5. コンフィグレーションファイルの保存先のフォルダを選択し、「保存」ボタンをクリックして、ファイルを保存します。
バックアップファイル名には、初期値（config.xml）を使用するか、または新しい名前を付けることができますが、必ず「.xml」拡張子を付けて保存してください。

Configuration Restore（コンフィグレーションのリストア）

本製品のファイル転送には、HTTP または TFTP を使用することができます。コンフィグレーションファイルを管理ステーションにダウンロードした後、XML フォーマットのコンフィグレーションファイルの編集を手動で行うことが可能です。編集したコンフィグレーションファイルは、本製品に再びアップロードして新たな設定を適用させることができます。

Maintenance > Configuration Restore の順にメニューをクリックします。本画面には、メインメニューから **Configuration > Configuration Restore** の順にクリックしてアクセスすることもできます。

TFTP を使用してコンフィグレーションをリストアする

1. 「Upload Method」の「TFTP」をチェックします。

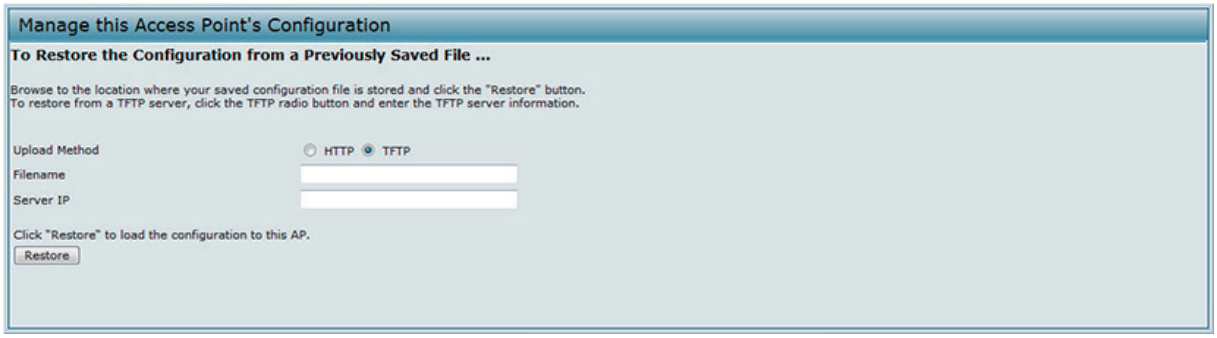


図 8-5　アクセスポイントのコンフィグレーションの管理 画面 - リストア（TFTP）

2. 「Filename」に、拡張子「.xml」のファイル名とファイルを保存するディレクトリへのパスを含むバックアップファイル名を入力します。

3. 「Server IP」に TFTP サーバの IP アドレスを入力します。

4. 「Restore」ボタンをクリックすると、コンフィグレーションのリストアが成功した後に、本製品が再起動する旨のダイアログが表示されます。

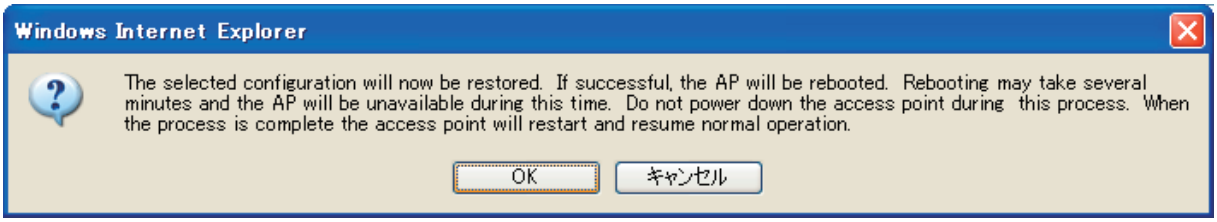


図 8-6　リストアの確認ダイアログ

5. 「OK」ボタンをクリックすると、本製品は再起動して経過が表示されます。

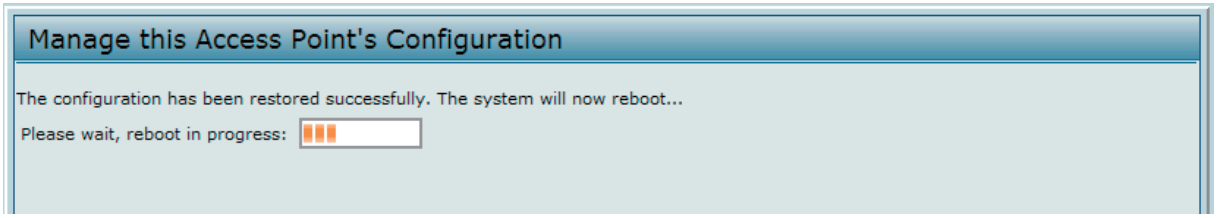


図 8-7　アクセスポイントのコンフィグレーションの管理 画面 - 経過表示

注意　再起動されるまで、数分かかることがあります。本製品が再起動されるまで、管理者用ユーザインタフェースにはアクセスできません。

HTTP を使用してコンフィグレーションをリストアする

1. 「Upload Method」の「HTTP」をチェックします。

図 8-8　アクセスポイントのコンフィグレーションの管理 画面 - リストア（HTTP）

2. 「参照」ボタンをクリックしてコンフィグレーションファイルがあるフォルダを開き、アップロードするファイルを選択して「開く」ボタンをクリックします。（リストアに使用できるファイルは、バックアップ機能で作成し、「.xml」形式で保存されたバックアップコンフィグレーションファイルだけです。例：ap_config.xml.）

3. 「Restore」ボタンをクリックすると、コンフィグレーションのリストアが成功した後に、本製品が再起動する旨のダイアログが表示されます。

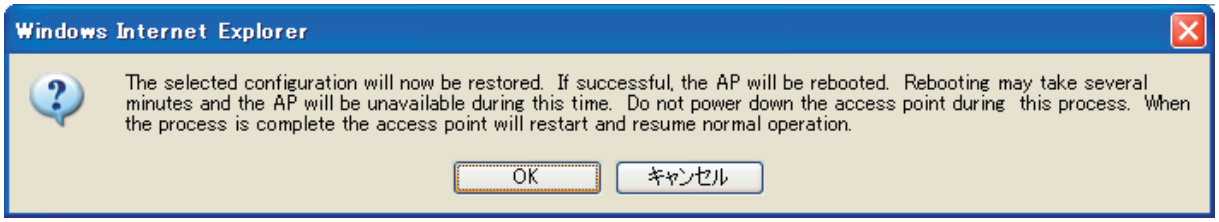


図 8-9　リストアの確認ダイアログ

4. 「OK」ボタンをクリックすると、本製品は再起動して経過が表示されます。

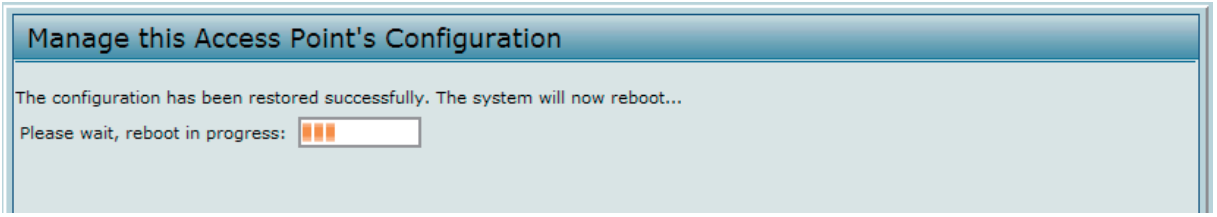


図 8-10　アクセスポイントのコンフィグレーションの管理 画面 - 経過表示

注意　再起動されるまで、数分かかることがあります。本製品が再起動されるまで、管理者用ユーザインタフェースにはアクセスできません。

Maintenance（リセットと再起動）

本製品を工場出荷時設定に戻すことや再起動を行うことができます。

Maintenance > **Maintenance** の順にメニューをクリックし、以下の画面を表示します。本画面には、ツールメニューから **System** をクリックしてアクセスすることもできます。

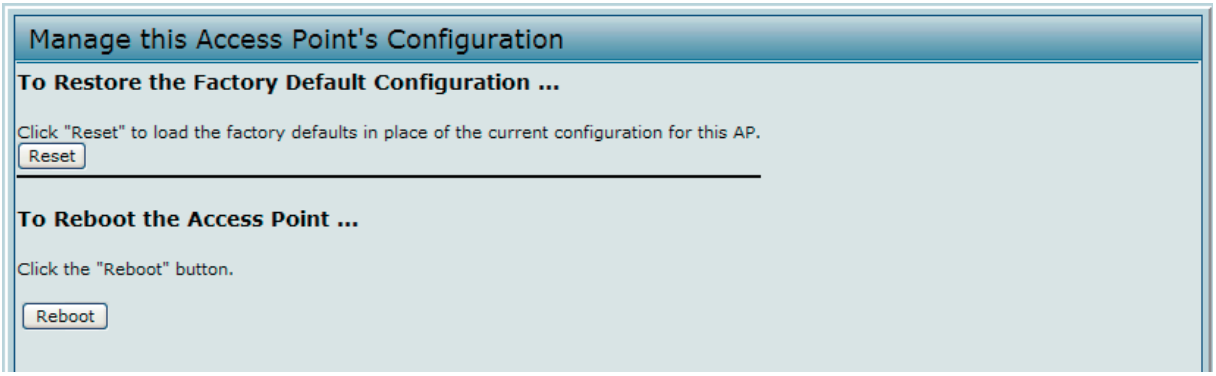


図 8-11　アクセスポイントのコンフィグレーションの管理 画面 - リセット & 再起動

工場出荷時の設定に初期化する

本製品の問題に対し、すべてのトラブルシューティングを試みても解決しなかった場合に使用します。「Reset」ボタンをクリックすると、設定を工場出荷時設定に戻す旨を示すダイアログが表示されます。

図 8-12　リセット確認ダイアログ

「OK」ボタンをクリックして本製品を工場出荷時設定に初期化します。パスワードや無線設定などを含むすべての設定が工場出荷時の設定に戻ります。本製品の背面にあるリセットボタンを押下して工場出荷時設定にリセットすることもできます。

本製品の再起動

メンテナンスまたはトラブルシューティングの方法として、本製品を再起動します。「Reboot」ボタンをクリックすると、本製品を再起動する旨のダイアログが表示されます。

図 8-13　再起動の確認ダイアログ

「OK」ボタンをクリックして本製品を再起動します。

Upgrade（ファームウェアの更新）

本製品ファームウェアの最新バージョンが利用可能になった場合、アップグレードして新しい機能や付加機能を得ることができます。ファームウェアのアップグレードには TFTP クライアントを使用することができます。また、HTTP も使用できます。

注意 ファームウェアを更新しても、本製品は既存の設定情報を保持します。

Maintenance > Upgrade の順にメニューをクリックします。本画面には、ツールメニューから **Tools > Upgrade** の順にクリックしてアクセスすることもできます。現在のファームウェアのバージョン情報が表示され、新しいファームウェアのアップグレードを行うオプションが提供されます。

TFTP を使用したファームウェアの更新

1. 「Upload Method」の「TFTP」をチェックします。

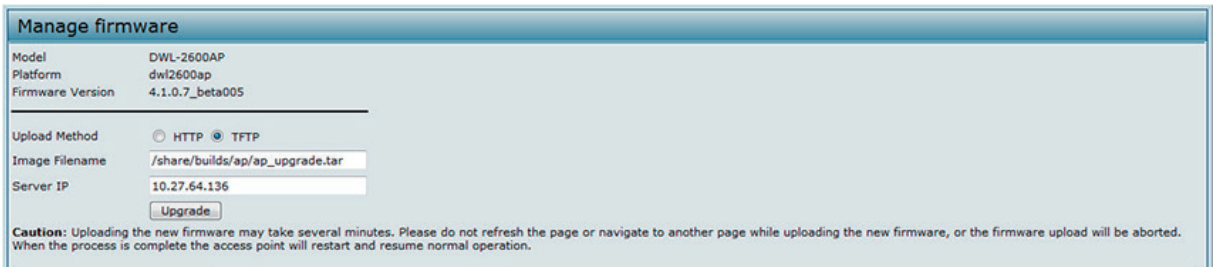


図 8-14　ファームウェアの更新 画面 - TFTP

2. 「Image Filename」欄に、アップロードするイメージのあるフォルダへのパスを含むイメージ名を入力します。
例えば、「/share/builds/ap」ディレクトリにある「ap_upgrade.tar image」をアップロードする場合は、「/share/builds/ap/ap_upgrade.tar」と入力します。

注意 ファームウェアのアップグレードには、tar 形式のファイルを使用する必要があります。bin ファイルやその他のフォーマットのファイルは使用しないでください。これらのタイプのファイルは動作しません。

3. 「Server IP」に TFTP サーバの IP アドレスを入力します。

4. 「Upgrade」ボタンをクリックすると、確認の画面が表示されアップグレードの処理を説明します。

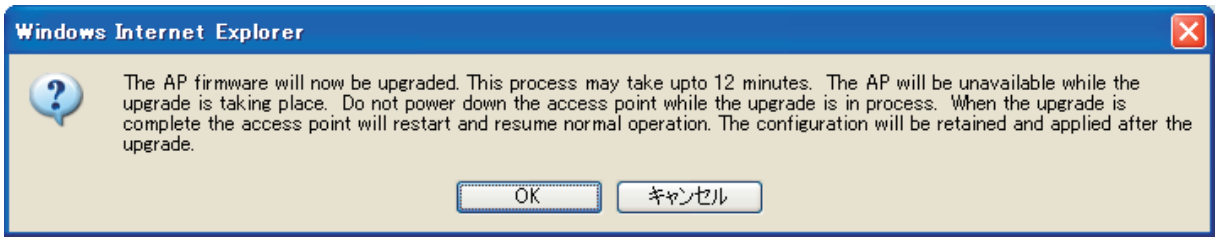


図 8-15　ファームウェアの更新確認ダイアログ

5. 「OK」ボタンをクリックして、アップグレードを開始します。経過画面が表示されますので、しばらくお待ちください。

注意 アップグレードには数分かかることがあり、その間本製品は使用できなくなります。アップグレードを行っている間は、本製品の電源を切らないでください。アップグレードが終了すると本製品は再起動されます。本製品は、アップグレード前と同じ設定で動作を開始します。

6. ファームウェアのアップグレードが正常に行われことを確認するためには、**Maintenance > Upgrade** メニューまたは **Basic Settings** メニューの「Firmware Version」を確認します。正常に行われた場合は、更新されたバージョン名または番号が表示されます。

HTTP を使用したファームウェアの更新

1. 「Upload Method」の「HTTP」をチェックします。

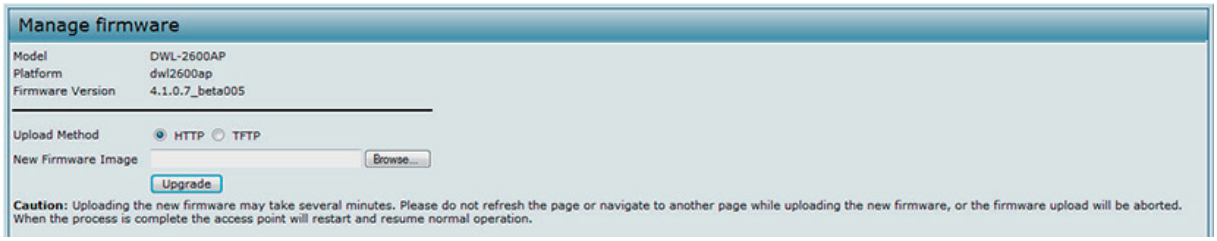


図 8-16　ファームウェアの更新 画面 - HTTP

2. ファイルへのパスがわかっている場合、「Image Filename」欄に入力します。不明な場合は、「参照」ボタンをクリックしてファームウェアイメージファイルを検出します。
ファームウェアのアップグレードには、tar 形式のファイルを使用する必要があります。bin ファイルやその他の形式のファイルは使用しないでください。これらのタイプのファイルは動作しません。

3. 「Upgrade」ボタンをクリックすると、確認の画面が表示されアップグレードの処理を説明します。

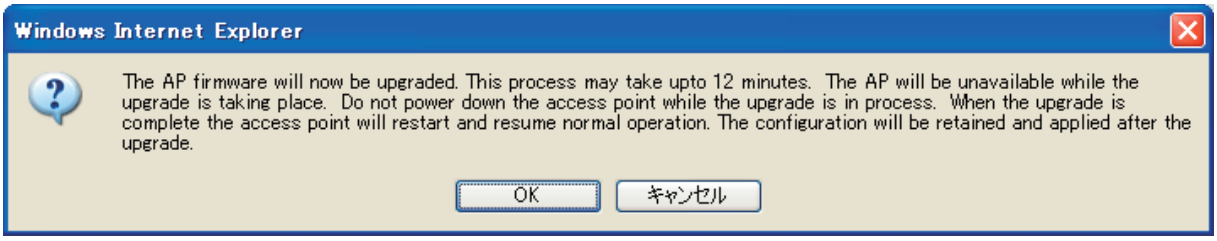


図 8-17　ファームウェアの更新確認ダイアログ

4. 「OK」ボタンをクリックして、アップグレードを開始します。経過画面が表示されますので、しばらくお待ちください。

注意 アップグレードには数分かかることがあり、その間本製品は使用できなくなります。アップグレードを行っている間は、本製品の電源を切らないでください。アップグレードが終了すると本製品は再起動されます。本製品は、アップグレード前と同じ設定で動作を開始します。

6. ファームウェアのアップグレードが正常に行われことを確認するためには、**Maintenance > Upgrade** メニューまたは **Basic Settings** メニューの「Firmware Version」を確認します。正常に行われた場合は、更新されたバージョン名または番号が表示されます。

Packet Capture（Packet Capture の設定）

無線パケットキャプチャは次の二つのモードで動作します。

- キャプチャファイルモード
- リモートキャプチャモード

キャプチャファイルモードでは捕捉されたパケットはファイルとしてアクセスポイントに保存されます。AP はファイルを TFTP サーバに送信することが可能です。ファイルは pcap フォーマットで保存され「Wireshark」や「OmniPeek」といったアプリケーションで使用可能です。

リモートキャプチャモードでは捕捉されたパケットは「Wireshark®」ツールを起動している外部 PC にリアルタイムで排出されます。

AP は次の種類のパケットを細くすることが可能です。:

- 無線インタフェースで送受信された 802.11 パケット。802.11 ヘッダを含む無線インタフェースで捕捉されたパケット。
- イーサネットインタフェースで送受信された 802.3 パケット。
- VAP や WDS インタフェースのような内部論理インタフェースで送受信された 802.3 パケット。

「Packet Capture Configuration」ページでできる設定は、:

- 現在のパケットキャプチャステータス
- パケットキャプチャ項目の設定
- パケットファイルキャプチャの設定
- リモートキャプチャポートの設定
- パケットキャプチャファイルのダウンロード

Maintenance > Packet Capture の順にメニューをクリックし、以下の画面を表示します。

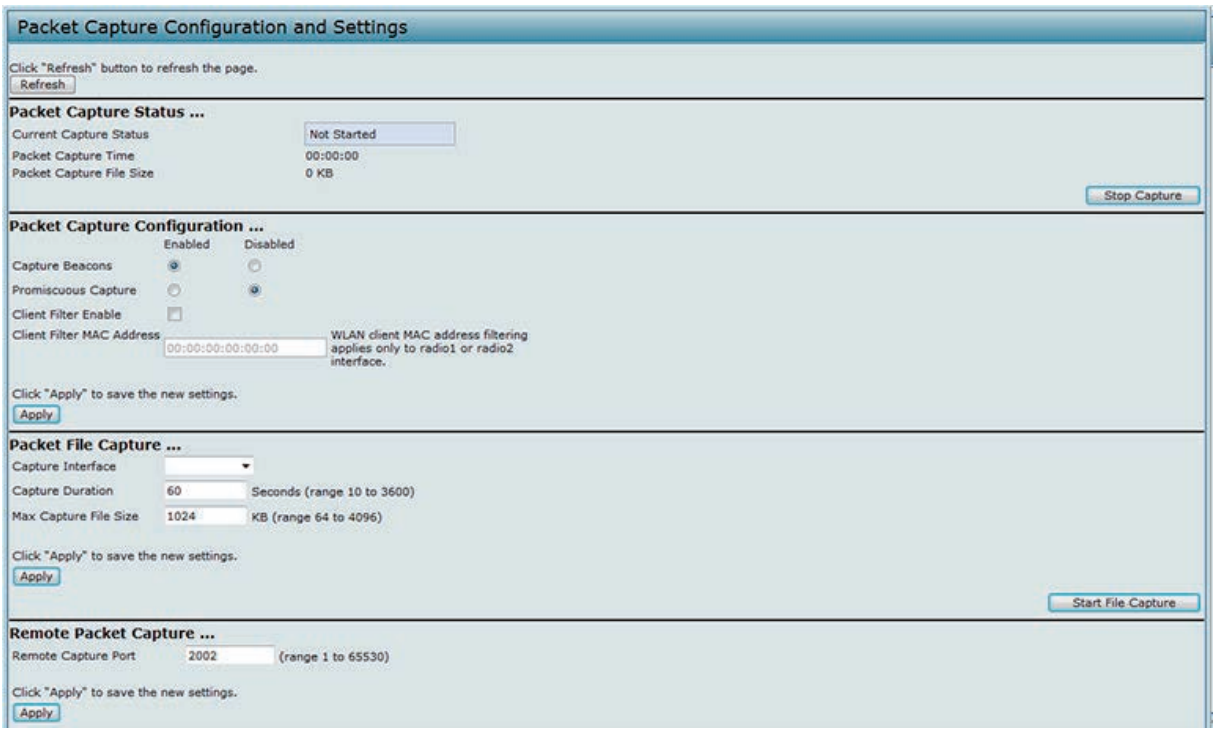


図 8-18　Packet Capture Configuration & Settings 画面

Packet Capture Status（パケットキャプチャステータス）

パケットキャプチャステータスで AP のパケットキャプチャの状態を表示します。

図 8-19　Packet Capture Status 画面

以下に示す項目を設定します。

項目	説明
Current Capture Status	パケットキャプチャの状態を表示します。
Packet Capture Time	パケットを補足した時間を表示します。
Packet Capture File Size	現在のキャプチャファイルの大きさを表示します。

Packet Capture Parameter Configuration（パケットキャプチャパラメータ設定）

パケットキャプチャパラメータの設定は無線インタフェースでのパケットキャプチャに関する設定を行います。

図 8-20　Packet Capture Configuration 画面

以下に示す項目を設定します。

項目	説明
Capture Beacons	無線で送信 / 検出された 802.11 ビーコンを捕捉します。
Promiscuous Capture	パケットキャプチャが有効の時に、「promiscuous」モードの無線を有効にします。 「promiscuous」モードでは無線は AP 宛に送信されていないトラフィックを含め。全てのチャンネル上のトラフィックを受信します。「promiscuous」モードで無線が動作している間でも、クライアントに足しては通常通りの動作を続けます。AP 宛ではないパケットは転送されません。キャプチャが完了すると、無線は「promiscuous」モードの動作から外れます。
Client Filter Enable	指定の MAC アドレスの無線クライアントから / への送受信フレームのみキャプチャするフィルタを有効にします。
Client Filter MAC Address	フィルタする無線クライアントの MAC アドレスを指定します。 **注意**　キャプチャが 802.11 インタフェースで作動している場合のみ、MAC フィルタは有効です。

注意　パケットキャプチャの設定項目を変更は、パケットキャプチャが再開した時に有効になります。パケットキャプチャセッションが行われている時の変更事項は、現行のパケットキャプチャでは適応されません。新しい設定項目を有効にするには、現在のパケットキャプチャセッションを一度止めて再開する必要があります。

Packet File Capture（パケットファイルキャプチャ）

パケットファイルキャプチャモードでは AP は捕捉したパケットをシステムの RAM に保存します。
動作中、パケットキャプチャは以下の事項が発生するまでパケットキャプチャを続けます。:

- 設定したキャプチャ時間が終了する。
- キャプチャファイルが最大サイズになる。
- 管理者がキャプチャを停止する。

キャプチャ中キャプチャステータスを確認することができます。「Refresh」をクリックすることで、経過時間、現在のキャプチャサイズなどの情報がアップデートされます。

図 8-21　Packet File Capture 画面

以下の項目が表示されます。

項目	説明
Capture Interface	AP キャプチャインタフェース名をドロップダウンメニューから選択します。 選択可能なパケットキャプチャ名は以下の通りです。: • 「brtrunk」- AP 内のリナックスブリッジインタフェースです。 • 「eth0」- イーサネットポートの 802.3 トラフィックです。 • 「wlan0」-「radio 1」の VAP0 トラフィックです。 • 「wlan1」-「radio 2」の VAP0 トラフィックです。 • 「radio1」-「radio 1」の 802.11 トラフィックです。 • 「radio2」-「radio 2」の 802.11 トラフィックです。
Capture Duration	キャプチャ期間を指定します。範囲は 10 から 3600 秒です。
Max Capture File Size	キャプチャファイルの最大限値です。64 から 4096KB です。

Remote Packet Capture（リモートパケットキャプチャ）

リモートパケットキャプチャはパケットキャプチャの宛先となるリモートポートを指定します。本機能は Windows のネットワーク分析ツールの「Wireshark」との共同作業となります。パケットキャプチャサーバは AP 上で動作し、TCP 接続を経由して「Wireshark」ツールへ捕捉パケットを送信します。
「Wireshark」が起動している Windows PC で捕捉されたトラフィックの表示、ログ、分析を行うことが可能です。

リモートキャプチャモードの使用中は AP はファイルシステムに捕捉データを保存することはありません。

一度に 5 つまでのインタフェースをトレースすることが可能です。しかしそれぞれのインタフェースで別々の「Wireshark」セッションを行う必要があります。AP と「Wireshark」を接続する IP ポート番号を設定することが可能です。ポート番号の初期値は「2002」です。システムは連続した 5 つのポート番号を使用し、パケットキャプチャのセッションを開始します。

「Wireshark」PC と AP の間にファイアウォールが設置されている場合、ポートはファイアウォールを通過できる必要があります。ファイアウォールはまた「Wireshark PC」と AP の TCP 接続を許可するように設定されている必要があります。

AP をキャプチャパケットの送信元として使用するように「Wireshark」を設定するには、「Capture Options」メニューのリモートインタフェースを設定する必要があります。例えば初期値の IP ポートを使用した「radio1」の IP アドレス「192.168.1.10」の AP の捕捉パケットの場合、次のようにインタフェースを指定します。:

rpcap://192.168.1.10/radio1

IP ポート「58000」を使用した「radio1」の「VAP0」の AP のイーサネットインタフェースでパケットを捕捉するためには、「Wireshark」セッションを二つ使用し、次のようにインタフェースを指定します。:

rpcap://192.168.1.10:58000/eth0
rpcap://192.168.1.10:58000/wlan0

無線インタフェースでトラフィックを捕捉している場合、ビーコンキャプチャは無効にできますが、他の 802.11 コントロールフレームは「Wireshark」へ送信されます。表示フィルタを以下の通りのみ設定できます。：

- トレース内のデータフレーム
- 指定した BSSID のトラフィック
- クライアント間のトラフィック

使用できる表示フィルタの例は以下の通りです。：

- 除外ビーコンと ACK/RTS/CTS フレーム：
- !(wlan.fc.type_subtype == 8 || wlan.fc.type == 1)

- データフレームのみ：
- wlan.fc.type == 2

- 指定の BSSID のトラフィック：
- wlan.bssid == 00:02:bc:00:17:d0

- 指定クライアントからの全トラフィック：
- wlan.addr == 00:00:e8:4e:5f:8e

リモートキャプチャモードではネットワークインタフェースの 1 つを経由し、「Wireshark」を起動している PC にトラフィックは送信されます。「Wireshark」の位置によってはトラフィックはイーサネットインタフェースや無線の 1 つに送信されることも可能です。トレースパケットによってトラフィック氾濫が発生するのを避けるために、AP は自動的に「Wireshark」アプリケーションを宛先にした全パケットをフィルタするキャプチャフィルタをインストールします。例えば、「Wireshark」IP ポートが「58000」に設定されている場合、AP に自動的にインストールされるキャプチャフィルタは次のようになります。：

not portrange 58000-58004.

パケットキャプチャ機能を有効にすることで AP パフォーマンスへの影響は、セキュリティ問題などがあります（無認証クライアントが AP に接続しユーザデータをトレースするなど）。AP との Wireshark セッションがなくても AP パフォーマンスへの悪い意味での影響はあります。パケットキャプチャが進行している時はパフォーマンスへの負の影響は広い範囲で発生します。

パフォーマンスとセキュリティ問題によって、パケットキャプチャモードは AP の NVRAM に保存されません。AP がリセットすると、キャプチャモードは無効になり、トラフィックをキャプチャするには再度有効にする設定を行わなければいけません。パケットキャプチャ項目は（モードではない）NVRAM に保存されます。

トラフィックキャプチャが進行中に AP へのパフォーマンスへの影響を最小限に抑えるためには、「Wireshark」ツールに送信するトラフィックに制限をかけるために、キャプチャフィルタをインストールすると有効です。802.11 トラフィックをキャプチャする時、捕捉されたフレームの大部分はビーコンへとなる傾向にあります。（通常全てのアクセスポイントにより 100ms 毎に送信されます。）「Wireshark」がビーコンフレーム用に表示フィルタをサポートしていても、「Wireshark」ツールへの捕捉されたビーコンパケットの転送から AP を防ぐキャプチャフィルタはサポートしていません。802.11 ビーコンのキャプチャによるパフォーマンスへの影響を削減するには、キャプチャビーコンモードを無効にすることも可能です。

リモートパケットキャプチャ機能は Windows の Wireshark ツールに標準搭載されています。

注意 リモートパケットキャプチャはリナックスバージョンの Wireshark では標準ではありません。リナックスバージョンは AP で動作しません。

「Wireshark」はオープンソースツールで無料で使用することが可能です。「http://www.wireshark.org」からダウンロードできます。

図 8-22　Remote Packet Capture 画面

以下の項目が表示されます。

項目	説明
Remote Capture Port	パケットキャプチャの宛先として使用されるリモートポートを指定します。範囲は 1 から 65530 です。

Packet Capture File Download（パケットキャプチャファイルのダウンロード）

パケットキャプチャファイルのダウンロードは TFTP によるキャプチャファイルを TFTP サーバまたは HTTP(S) から PC へダウンロードすることです。キャプチャされたパケットは AP の「file /tmp/apcapture.pcap」内に保存されます。キャプチャファイルのダウンロードコマンドを引き金に、キャプチャは自動的に停止します。キャプチャファイルは RAM ファイルシステムに保存されるため、AP がリセットされると消滅します。

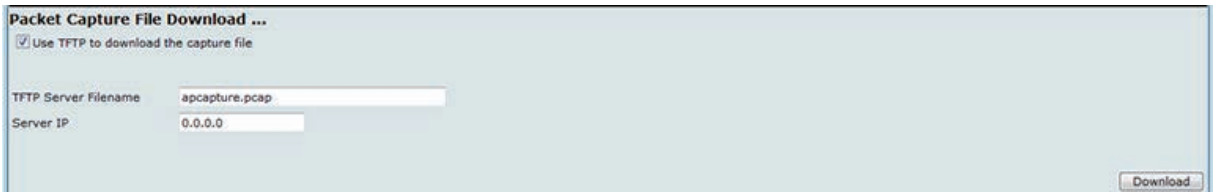


図 8-23　Packet Capture File Download 画面

以下の項目が表示されます。

項目	説明
Use TFTP to download the capture file	キャプチャファイルのダウンロードに「TFTP」または「HTTP(S)」のどちらを使用するか選択 / 解除します。: • 「TFTP」を使用してダウンロードする場合、選択し残りの項目を設定します。 • 「HTTP/HTTPs」を使用してダウンロードする場合、オプションをクリアし、「Download」をクリック、ファイルの保存場所を参照します。
TFTP Server Filename	「TFTP」でファイルをダウンロードする場合、「.pcap」ファイル名、保存場所のディレクトリパスを含んだパケットキャプチャファイル名を指定します。
Server IP	「TFTP」を使用してダウンロードする場合、TFTP サーバの IP アドレスを指定します。

第 9 章　Client QoS（クライアント QoS の設定）

無線クライアントからアクセスポイントへのトラフィックに作用する QoS の設定方法について説明します。統合アクセスポイントのクライアント QoS 機能を使用して、帯域制限を行い、無線インタフェースにアクセスコントロールリストおよび DiffServ ポリシーを適用することができます。

設定項目	説明	参照ページ
VAP QoS Parameters（VAP QoS パラメータの設定）	ネットワークに接続する無線クライアントの QoS に個々のクライアントが送受信を許可される帯域幅のコントロールを行います。	112 ページ
Managing Client QoS ACL（クライアント QoS ACL の管理）	アクセスコントロールリストは、特定のリソースにアクセスする非認証のユーザを防ぎ、認証されたユーザに許可を与えて、安全性を提供します。	113 ページ
Class Map（Diffserv クラスマップ の作成）	DiffServ クラスマップを作成します。	120 ページ
Policy Map（Diffserv ポリシーマップの作成）	Diffserv ポリシーマップを作成します。	125 ページ
Client QoS Status（クライアント QoS ステータス）	接続クライアントの QoS 設定を参照します。	127 ページ
Configuring RADIUS-Assigned Client QoS Parameters（RADIUS クライアント QoS パラメータ）	RADIUS クライアントデータベースに参照される ACL と DiffServ ポリシーは無線クライアントに適用するために、必ず ACL 名と AP で設定された DiffServ ポリシー に合致する必要があります。	128 ページ

本章におけるこれらの機能の設定画面は、Web ユーザインタフェースのメインメニューから「Client QoS」をクリックして表示します。

VAP QoS Parameters（VAP QoS パラメータの設定）

本製品のクライアント QoS 機能は、ネットワークに接続する無線クライアントの QoS に、個々のクライアントが送受信を許可される帯域幅のコントロールなどのさらに詳細な制御を提供します。HTTP トラフィックや特定サブネットからのトラフィックなどの一般的なカテゴリのトラフィックを制御するために、アクセスコントロールリストを設定し、1 つ以上の VAP に割り当てることができます。

一般的なカテゴリのトラフィックの制御に加え、クライアントの QoS では、各クライアントが DiffServ による様々なマイクロフロー調整を行うように設定することができます。DiffServ ポリシーは、ネットワーク上で内向きと外向き両方のトラフィックを認証する時に、各無線クライアントに適用する一般的なマイクロフロー定義および特性処理を確立するのに役立つツールです。

クライアントの Client QoS 機能を有効にして、クライアントの帯域制限を指定し、VAP に接続するクライアントが RADIUS サーバによって定義される属性を持たない場合、アクセスコントロールリストおよび DiffServ ポリシーを選択して初期値として使用します。

クライアント QoS の管理モードを設定し、VAP の QoS 設定を行います。

Client QoS > VAP QoS Parameters の順にメニューをクリックし、以下の画面を表示します。

図 9-1　クライアント QoS の VAP 設定 画面

画面には以下の項目があります。

項目	説明
Client QoS Global Admin Mode	アクセスポイントのクライアント QoS 機能を有効または無効にします。本設定を変更しても、QoS 画面で行った WMM 設定は変更されません。
Radio	「1」または「2」を選択して設定する無線インタフェースを指定します。
VAP	クライアント QoS 設定を行う VAP（VAP 0-15）を指定します。指定した VAP に設定した QoS は、他の VAP 経由でネットワークに接続しているクライアントには適用されません。
Client QoS Mode	VAP メニューから選択した VAP の QoS 機能を有効または無効にします。 クライアント QoS 設定を無線クライアントに適用するためには、「Client QoS Global Admin Mode」欄でグローバルに有効にし、さらに本欄の VAP を有効にする必要があります。
Bandwidth Limit Down	アクセスポイントから無線クライアントへの最大送信速度（bps）を入力します。範囲は 0-4294967295（bps）です。 0 以外の値を指定すると、アクセスポイントが使用できるように 64 Kbps に近くなるように丸められますが、64 Kbps 未満になることはありません。0 は、最大帯域幅制限が実施されないことを意味します。
Bandwidth Limit Up	無線クライアントからアクセスポイントへの最大送信速度（bps）を入力します。範囲は 0-4294967295（bps）です。0 以外の値を指定すると、アクセスポイントが使用できるように 64 Kbps に近くなるように丸められますが、64 Kbps 未満になることはありません。0 は、最大帯域幅制限が実施されないことを意味します。
ACL Type Down	外向きトラフィックに適用するアクセスコントロールリストのタイプ（NONE または IPv4）を選択します。「IPv4」を選択すると、アクセスコントロールリストは、アクセスコントロールリストのルールに一致する IPv4 パケットを検証します。
ACL Name Down	外向きトラフィックに適用するアクセスコントロールリスト名を選択します。パケットが外向きのインタフェースに変更されると、一致するアクセスコントロールリストが確認されます。パケットは、許可された場合には送信され、拒否されると廃棄されます。

項目	説明
ACL Type Up	内向きトラフィックに適用するアクセスコントロールリストのタイプ（NONE または IPv4）を選択します。「IPv4」を選択すると、アクセスコントロールリストは、ACL ルールに一致する IPv4 パケットを検証します。
ACL Name Up	内向きトラフィックに適用するアクセスリスト名を選択します。アクセスポイントがパケットやフレームを受信すると、一致するアクセスコントロールリストをチェックします。パケットやフレームは、許可されると送信され、拒否された場合には廃棄されます。
DiffServ Policy Down	外向きトラフィックに適用する DiffServ ポリシー名を選択します。
DiffServ Policy Up	内向きトラフィックに適用する DiffServ ポリシー名を選択します。

「Apply」ボタンをクリックして設定を適用します。

Managing Client QoS ACL（クライアント QoS ACL の管理）

アクセスコントロールリストは、許可と廃棄の条件をまとめたものであり、特定のリソースにアクセスする非認証のユーザを防ぎ、認証されたユーザに許可を与えて、安全性を提供します。アクセスコントロールリストは、どんなネットワークリソースへの不正なアクセスも防ぐことができます。

本製品は IPv4 、IPv6、MAC アクセスコントロールリストをサポートしています。

IPv4 /IPv6 アクセスコントロールリスト

IP アクセスコントロールリストは、レイヤ 3 およびレイヤ 4 のトラフィックを分類します。各アクセスコントロールリストは最大 10 個のルールの集まりで、無線クライアントから送信されたトラフィックや無線クライアントに送信されるトラフィックに適用されます。各ルールは各欄のコンテンツを使用して、ネットワークへの接続を許可するべきか、拒否するべきかを指定します。ルールはさまざまな基準に基づくことができ、送信元および送信先 IP アドレス、レイヤ 4 ポート、あるいは、パケットが運ぶプロトコルなど、パケット内の複数のフィールドに適用することが可能です。

MAC アクセスコントロールリスト

MAC アクセスコントロールリストはレイヤ 2 ACL です。宛先 / 送信元 MAC アドレス、VLAN ID、Class of Service 802.1p priority などのフレームの項目検査のルールを設定できます。フレームが AP ポートに入る / 出る時（ACL が「up」または「down」のどちらかに設定されているかに依存する。）、AP はフレームを検査し、ACL ルールがフレームの内容に違反していないかチェックします。もしルールが 1 つでも内容に合致している場合「permit」または「deny」の動作がフレームに対して行われます。

アクセスコントロールリストの設定手順

アクセスコントロールリストおよびルールの設定を行い（手順 1-5）、特定の VAP にルールを適用します（手順 6、7）。

アクセスコントロールリストの一般的な設定手順は以下の通りです。

1. **Client QoS > Client QoS ACL** の順にメニューをクリックし、以下の画面を表示します。

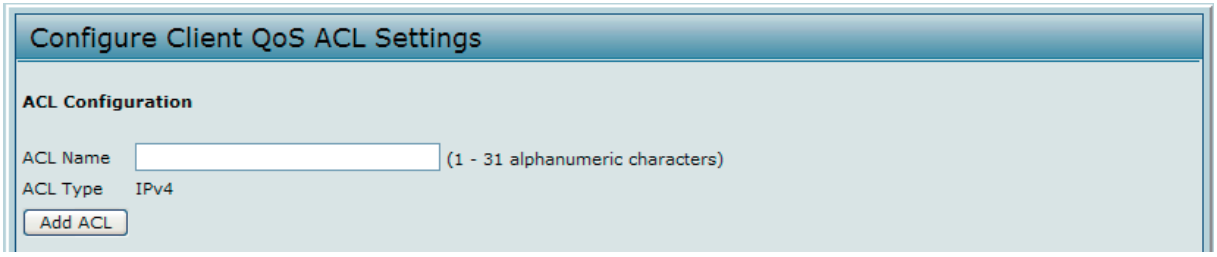


図 9-2　クライアント QoS の ACL 設定 画面

2. アクセスコントロールリストの名前を指定し、「Add ACL」ボタンをクリックすると、以下のルール設定項目が表示されます。

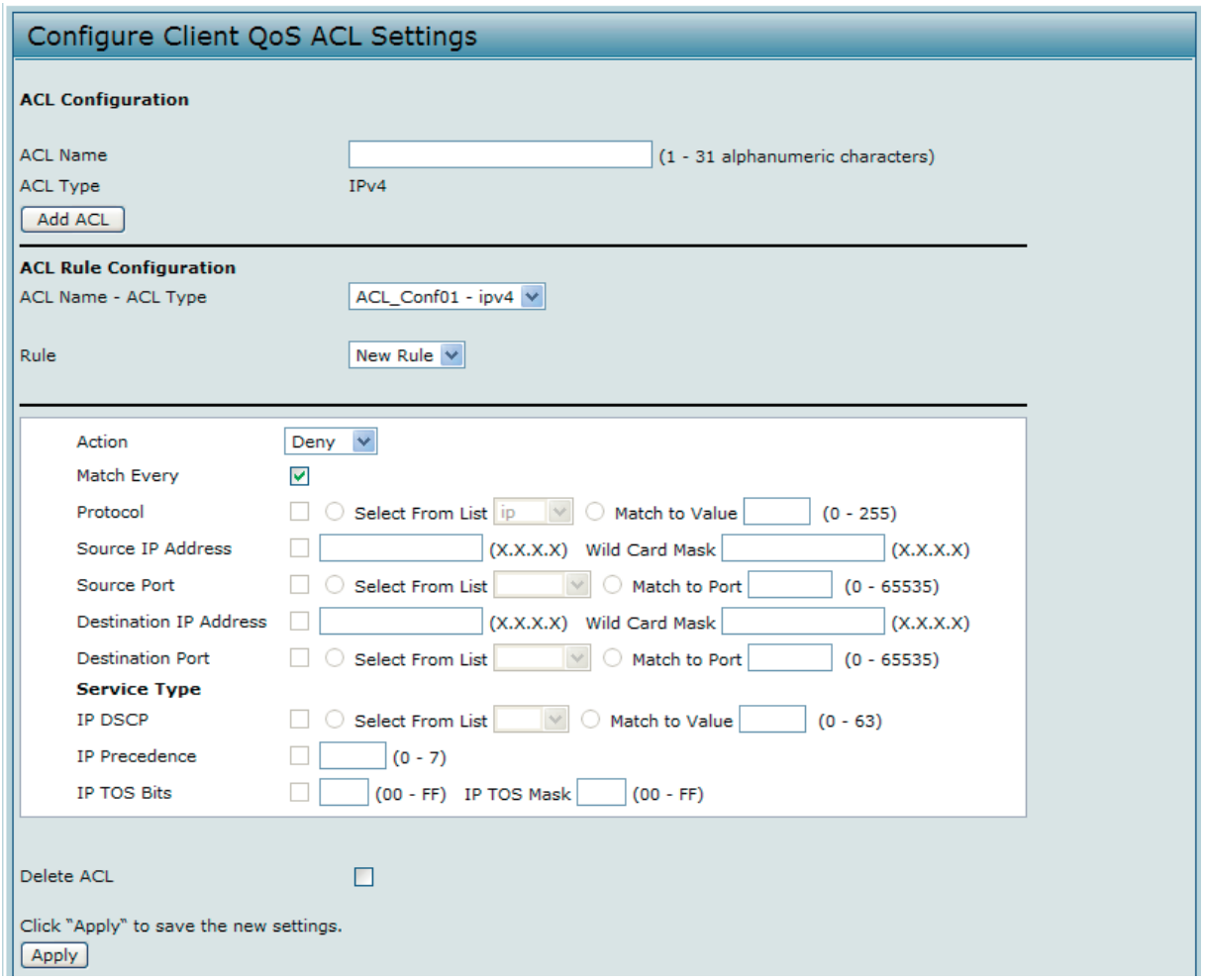


図 9-3　クライアント QoS の ACL 設定 画面 - ルール設定

3. 「ACL Name - ACL Type」にルールを設定するアクセスコントロールリストを選択します。

4. 新しいルールを設定するために、「Rule」で「New Rule」を選択します。

5. ルールの照合基準を設定し、「Apply」ボタンをクリックしてルールを作成します。

6. 作成したアクセスコントロールリストを 1 つ以上の VAP に適用します。
Client QoS > VAP QoS Parameters の順にメニューをクリックし、以下の画面を表示します。

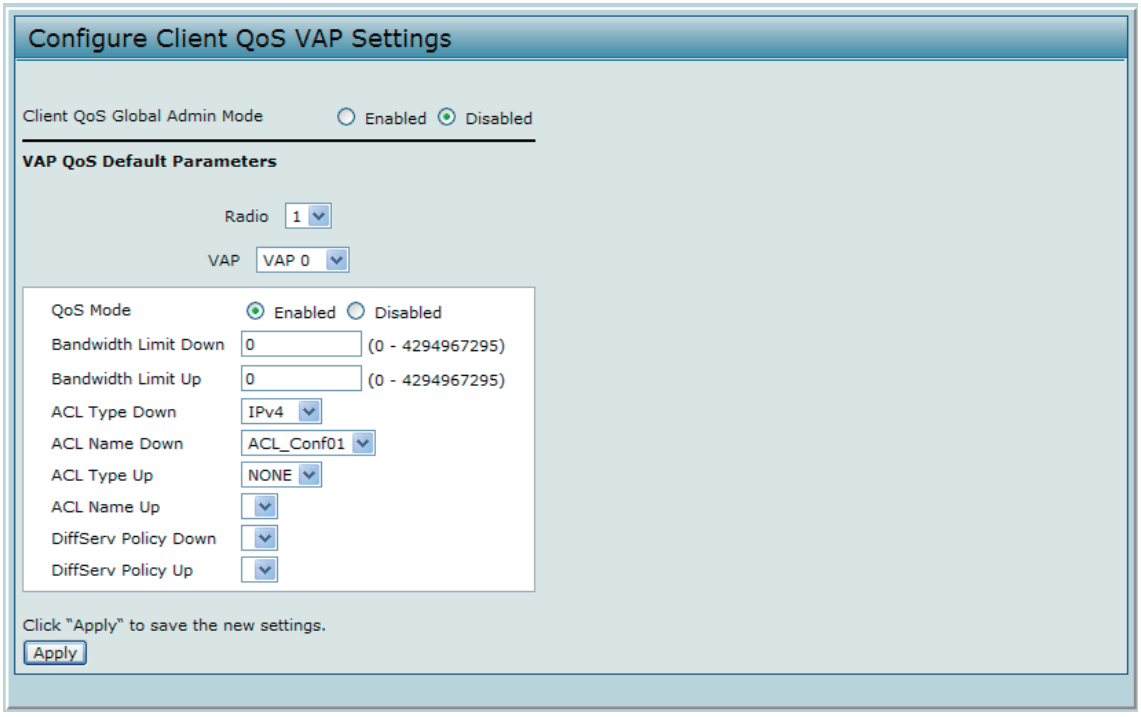


図 9-4　クライアント QoS VAP 設定 画面

7. 「QoS Mode」で「Enabled」、「ACL Type Down」または「ACL Type Up」で「IPv4」を選択後に「ACL Name Down」または「ACL Name Up」で ACL を選択します。

以下の表に「Client QoS ACL」画面の各項目の詳細を示します。

項目	説明
ACL Configuration	
ACL Name	アクセスコントロールリストの名称（最大 31 文字の半角英数字）を入力します。空白は使用できません。
ACL Type	設定する ACL のタイプを指定します。 • IPv4 • IPv6 • MAC IPv4/IPv6 ACL は L3 と L4 の基準を元にネットワークリソースへのアクセスをコントロールします。 MAC ACL は L2 基準を元にアクセスコントロールを行います。
ACL Rule Configuration	
ACL Name - ACL Type	新しいルールを設定する ACL 名を指定します。ここには「ACL Configuration」セクションで作成したすべての ACL が表示されます。
Rule	「New Rule」を指定して、選択した ACL に追加する新しいルールを設定します。ACL への既存ルールの追加、またはルールの変更を行う時は、そのルール番号を選択します。ACL 内の複数のルールは、ACL に追加した順番でパケットに適用されます。最終ルールとして、「implicit deny all rule」（暗黙の全否定）があります。
Action	ACL ルールが許可または拒否するアクションを指定します。 • Permit - 指定する ACL の指示に従って、そのルールが決めるアクセスポイントへの送受信の基準に一致するトラフィックはすべて許可されます。基準に合わないトラフィックはすべて廃棄されます。 • Deny - 指定する ACL の指示に従って、そのルールが決めるアクセスポイントへの送受信の基準に一致するトラフィックをすべて拒否します。基準に合わないトラフィックはすべて送信されますが、最終ルールの場合は異なります。各 ACL の最後には「implicit deny all rule」（暗黙の全否定）という最終ルールがあり、明らかに許可されたトラフィック以外は廃棄されるます。
Match Every	許可または拒否いずれかのアクションを持つルールを、パケットのコンテンツに関わらず一致させるよう指示します。選択すると、照合基準を追加設定することはできません。新しいルールは初期値で「Match Every」オプションが選択されます。他の照合基準を設定するためには、本オプションを必ず外して下さい。
IPv4 ACL	

項目	説明
Protocol	本欄を指定して、IPv4 パケットの IP プロトコルフィールドの値に基づいて使用するレイヤ 3 またはレイヤ 4 プロトコルの一致条件を選択します。チェックした後、キーワードまたはプロトコル ID を入力して一致させるプロトコルを選択します。 • Select From List 本リストからプロトコルを 1 つ選択します。 - ip - icmp - igmp - tcp - udp • Match to Value 名前にないプロトコルに一致させる時はプロトコル ID を入力します。プロトコル ID は、IANA によって割り当てられたプロトコル番号です。範囲は 0-255 です。
Source IP Address	これを選択すると、パケットの送信元 IP アドレスがここに登録されているアドレスに一致するよう要求します。この基準を適用する IP アドレスを入力します。
Wild Card Mask	送信元 IP アドレスをワイルドカードマスクに指定します。 ワイルドカードマスクは、一致させるビットと無視するビットを決定するものです。「255.255.255.255」のワイルドカードマスクは、すべてのビットを無視することを示します。ワイルドカードが「0.0.0.0」の場合は、すべてのビットを一致させることを示します。本欄は、「Source IP Address」ボックスがチェックされている場合にのみ入力します。 ワイルドカードマスクは、実際にはサブネットマスクを逆（ビット反転したもの）にします。例えば、シングルホストアドレスに基準を一致させる場合は、ワイルドカードマスク「0.0.0.0.」を使用します。24 ビットのサブネット（例：192.168.10.0/24）に基準を一致させる時は、評価基準を合わせるために、「0.0.0.255」のワイルドカードマスクを使用します。
Source Port	ルールの一致条件に送信元ポートを含める場合に選択します。送信元ポートはデータグラムヘッダで識別します。ポート名を指定するか、またはポート番号を入力します。 • Select From List 一致させる送信元ポートに関連するキーワードを選択します。 - ftp - ftpdata - http - smtp - snmp - telnet - tftp - www 各キーワードは相当するポート番号に変換されます。 • Match to Port データグラムヘッダで識別される送信元ポートに一致させる IANA ポート番号を入力します。ポート範囲は 0-65535 で、以下の 3 つの異なるポートタイプを含みます。 - 0-1023：通常のポート - 1024-1518：登録されたポート - 49152-65535：ダイナミックおよび / またはプライベートポート
Destination IP Address	本欄を選択すると、パケットの送信先 IP アドレスがここに登録されているアドレスに一致するよう要求します。この基準を適用する IP アドレスを入力します。
Wild Card Mask	送信先 IP アドレスをワイルドカードマスクに指定します。 ワイルドカードマスクは、一致させるビットと無視するビットを決定するものです。「255.255.255.255」のワイルドカードマスクは、すべてのビットを無視することを示します。ワイルドカードが「0.0.0.0」の場合は、すべてのビットを一致させることを示します。本欄は、「Destination IP Address」ボックスがチェックされている場合にのみ入力します。 実際にはサブネットマスクを逆（ビット反転したもの）にします。例えば、シングルホストアドレスに基準を一致させる場合は、ワイルドカードマスク「0.0.0.0.」を使用します。24 ビットのサブネット（例 :192.168.10.0/24）に基準を一致させる時は、評価基準を合わせるために、「0.0.0.255」のワイルドカードマスクを使用します。

項目	説明
Destination Port	ルールの一致条件に送信先ポートを含める場合に選択します。送信先ポートはデータグラムヘッダで識別します。ポート名を指定するか、またはポート番号を入力します。 • Select From List 一致させる送信先ポートに関連するキーワードを選択します。 - ftp - ftpdata - http - smtp - snmp - telnet - tftp - www 各キーワードは相当するポート番号に変換されます。 • Match to Port データグラムヘッダで識別される送信先ポートに一致させる IANA ポート番号を入力します。ポート範囲は 0-65535 で、以下の 3 つの異なるポートタイプを含みます。 - 0-1023 : 通常のポート - 1024-1518 : 登録されたポート - 49152-65535 : ダイナミックおよび / またはプライベートポート
Service Type	
IP DSCP	一致基準として IP DSCP を使用するためには、チェックボックスを選択し、DSCP 値のキーワードを選択するか、または DSCP を入力します。 • Select from List - DSCP タイプのリスト（af11-12、af21-23、af31-33、af41-43、cs0-7、ef）から選択します。 • Match to Value - 照合する DSCP 値（0-63）を入力します。
IP Precedence	本欄を選択すると、パケットの「IP Precedence」値をクラス基準の IP Precedence 値と照合します。IP Precedence 範囲は 0-7 です。
IP TOS Bits	一致基準として使用するパケットの IP ヘッダのサービスタイプのビット値を入力します。パケット内の IP TOS フィールドは、IP ヘッダの「Service Type」オクテットの全 8 ビットとして定義されます。この値は、00-FF までの 2 桁の 16 進数です。上位 3 ビットは IP 優先度値を表します。上位 6 ビットは IP Differentiated Services Code Point（DSCP）値を表します。
IP TOS Mask	IP TOS マスク値を入力し、パケットの「IP TOS」フィールドと比較するために使用される TOS ビット値内のビット位置を指定します。TOS マスク値は、00 ～ ff までの 2 桁の 16 進数で、逆（つまり、ワイルドカード）マスクを表します。「TOS Mask」内の「0」の値は、パケットの「IP TOS」フィールドと比較するために使用される TOS ビット値のビット位置を指定します。例えば、ビット 7（ビット 7 は非常に重要です。）と 5 を設定した IP TOS 値をチェックし、ビット 1 をクリアするためには、TOS ビット値「0xA0」と TOS Mask「0xFF」を使用します。これはオプション設定です。
IPv6 ACL	
Protocol	本欄を指定して、IPv4 パケットの IP プロトコルフィールドの値、または IPv6 パケットのネクストパケットフィールドに基づいて使用するレイヤ 3 またはレイヤ 4 プロトコルの一致条件を選択します。 チェックした後、キーワードまたはプロトコル ID を入力して一致させるプロトコルを選択します。 **Select From List** 次のリストのプロトコルから一つを選択します。: • IP • ICMP • IPv6 • ICMPv6 • IGMP • TCP • UDP **Match to Value** 名前でリストにマッチするプロトコルがない場合、プロトコル ID を入力します。 プロトコル ID は IANA によってアサインされた通常値です。範囲は「0–255」になります。
Source IPv6 Address	パケットの送信元 IPv6 アドレスをリストのアドレスにマッチさせるために、本フィールドを選択します。 正しいフィールドに IPv6 アドレスを入力します。
Source IPv6 Prefix Length	送信元 IPv6 アドレスのプリフィクス長を入力します。

項目	説明
Source Port	ルールにマッチした状態の送信元ポートを含むために本オプションを選択します。送信元ポートはデータグラムヘッダで識別されます。 このフィールドを選択するとポート名の選択やポート番号の入力をします。: • Select From List 一致させる送信元ポートに関連するキーワードを選択します。 • ftp • ftpdata • http • smtp • snmp • telnet • tftp • www 各キーワードは相当するポート番号に変換されます。 • Match to Port データグラムヘッダで識別される送信元ポートに一致させる IANA ポート番号を入力します。 ポート範囲は 0-65535 で、以下の 3 つの異なるポートタイプを含みます。 - 0-1023 : 通常のポート - 1024-1518 : 登録されたポート - 49152-65535 : ダイナミックおよび / またはプライベートポート
Destination IPv6 Address	本欄を選択すると、パケットの送信先 IPv6 アドレスがここに登録されているアドレスに一致するよう要求します。この基準を適用する IP v6 アドレスを入力します。
Destination IPv6 Prefix Length	送信先 IPv6 アドレスのプリフィクス長を入力します。
Destination Port	ルールの一致条件に送信先ポートを含める場合に選択します。送信先ポートはデータグラムヘッダで識別します。ポート名を指定するか、またはポート番号を入力します。 • Select From List 一致させる送信先ポートに関連するキーワードを選択します。 - ftp - ftpdata - http - smtp - snmp - telnet - tftp - www 各キーワードは相当するポート番号に変換されます。 • Match to Port データグラムヘッダで識別される送信先ポートに一致させる IANA ポート番号を入力します。ポート範囲は 0-65535 で、以下の 3 つの異なるポートタイプを含みます。 - 0-1023 : 通常のポート - 1024-1518 : 登録されたポート - 49152-65535 : ダイナミックおよび / またはプライベートポート
IPv6 Flow Label	フローラベルは IPv6 パケットにとって固有の 20 ビットの番号です。ルータ内の QoS に対応するエンドステーションによって使用されます。範囲は 0 から 1048575 です。
IPv6 DSCP	ルールの一致条件に IPv6 DSCP を含める場合に選択します。 キーワードまたは DSCP 値を入力します。ルールの一致条件としてサービスタイプを 1 つのみ選択できます。 「DSCP」「IP Precedence」「TOS bits」など • Select From List DSCP の種類を選択します。 • Match to Value DSCP 値を入力します。(0 – 63)

項目	説明
MAC ACL	
EtherType	ルールの一致条件に EtherTypw を含める場合に選択します。Ethernet Frame ヘッダで識別します。 • Select From List 一致させる EtherType に関連するキーワードを選択、または EterType 値を入力します。 - appletalk - arp - ipv4 - ipv6 - ipx - netbios - pppoe • Match to Port パケットに一致するカスタムプロトコルを入力します。16 進数の 4 文字で範囲は「0600 – FFFF」。
Class of Service	本欄を選択し、イーサネットフレームと照合する CoS 802.1p ユーザ優先度値を入力します。値の範囲は 0-7 です。
Source MAC Address	本欄を選択し、Ethernet フレームと比較する送信元 MAC アドレスマスクを入力します。
Source MAC Mask	Ethernet フレームと比較する送信元 MAC のビット位置を指定する送信元 MAC アドレスマスクを入力します。
Destination MAC Address	本欄を選択し、Ethernet フレームと比較する送信先 MAC アドレスマスクを入力します。
Destination MAC Mask	Ethernet フレームと比較する送信先 MAC のビット位置を比較する送信先 MAC アドレスマスクを入力します。
VLAN ID	本欄を選択し、イーサネットフレームと比較する VLAN ID を入力します。VLAN ID の範囲は 0-4095 です。

After you set the desired rule criteria, click Apply. To delete an ACL, select the Delete ACL option and click Apply.

ACL の削除

Client QoS > Client QoS ACL 画面で、「Rule」から削除するルール番号を選択します。次に「Delete ACL」をチェックして、「Apply」ボタンをクリックします。

Class Map（Diffserv クラスマップの作成）

クライアントの QoS は、Differentiated Services（DiffServ）をサポートしており、トラフィックを定義済みのホップ単位の動作に基づいてをストリームに分類して、特定の QoS 処理を行うことができます。

標準の IP ベースのネットワークは、「最適な」データ送信サービスを提供するために設計されています。「最適な」サービスは、ネットワークがデータをタイムリーに送信することを意味しますが、保証はありません。輻輳状態の場合には、パケットには遅延、散発的な送信、破棄が起こるかもしれません。E-mail およびファイル転送などの代表的なインターネットアプリケーションでは、サービスのわずかな低下は容認され、多くの場合気づかれません。逆に、音声またはマルチメディアなどの厳しいタイミング要求を持つアプリケーションでは、サービスの低下は望ましくない結果をもたらします。

トラフィックを分類し、これらのトラフィッククラスを処理する方法を定義するポリシーを作成することによって、時間に厳しいトラフィックに他のトラフィックより高い優先度を確実に与えることができます。

Diffserv クラスマップの定義

クライアント QoS に DiffServ を使用するためには、「Class Map」と「Policy Map」画面を使用して以下のカテゴリとそれらの基準を定義します。

- クラス - クラスを作成し、クラスの基準を定義します。
- ポリシー - ポリシーを作成し、ポリシーにクラスを関連付けてポリシーのステートメントを定義します。

一度、クラスを定義して、ポリシーにそれを関連付けたら、**Client QoS > VAP QoS Parameters** 画面で指定した VAP にポリシーを適用します。

パケットは、定義した基準に基づいて分類されて、処理されます。分類の基準はクラスによって定義されます。その処理はポリシーの属性によって定義されます。ポリシーの属性はクラスごとにインスタンスベースで定義し、これらの属性は一致する場合に適用されます。ポリシーには、複数のクラスを含めることができます。ポリシーがアクティブな場合は、パケットがどのクラスに一致するかによって、アクションを行います。

パケット処理は、パケットに対してクラスの基準に一致するかどうかをテストすることで開始します。そのポリシーで一致するクラスが見つかると、ポリシーがパケットに適用されます。DiffServ は IPv4 と IPv6 パケットにサポートされています。

新しい Diffserv クラス名の追加、既存のクラス名の変更または削除を行います。また、DiffServ クラスに割り当てる基準を定義します。

1. **Client QoS > Class Map** の順にメニューをクリックし以下の画面を表示します。

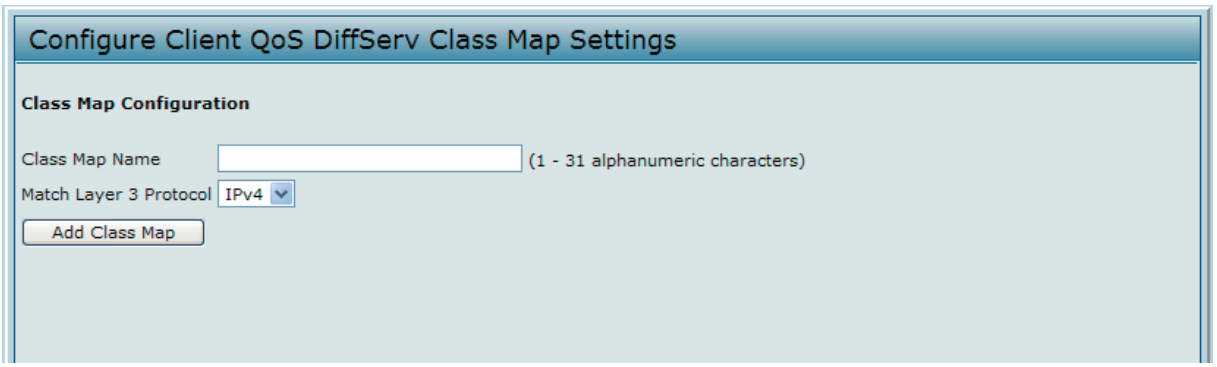


図 9-5　クライアント QoS DiffServ クラスマップ設定 画面

2. 新しいクラスマップを作成するためには、「Class Map Name」にクラスマップ名、「Match Layer 3 Protocol」にプロトコル（IPv4 または IPv6）を指定して「Add Class Map」ボタンをクリックします。クラスマップが作成されると、「Class Map」画面には「Match Criteria Configuration」欄が表示されます。

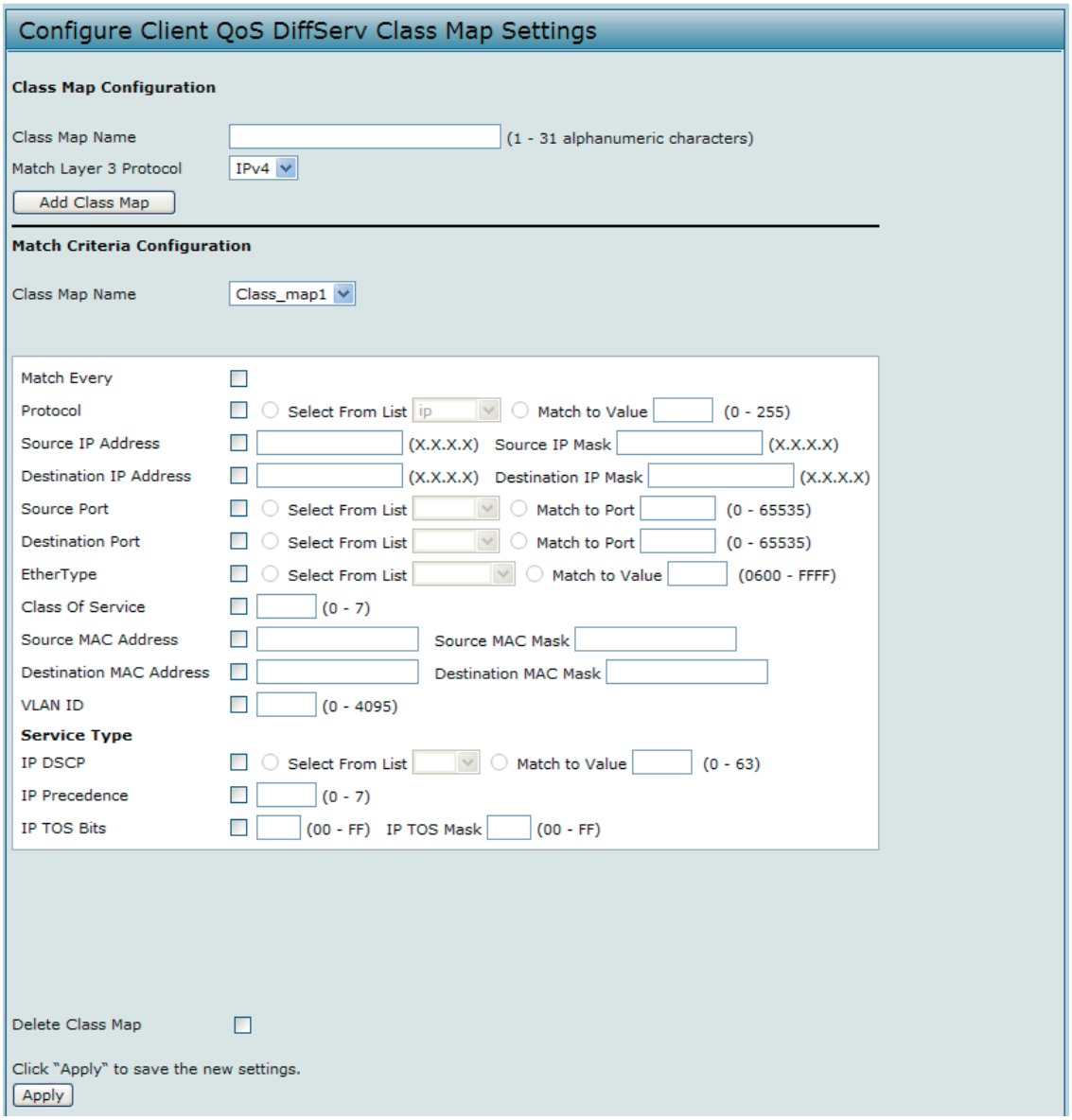


図 9-6　クライアント QoS DiffServ クラスマップ設定 画面 - IPv4

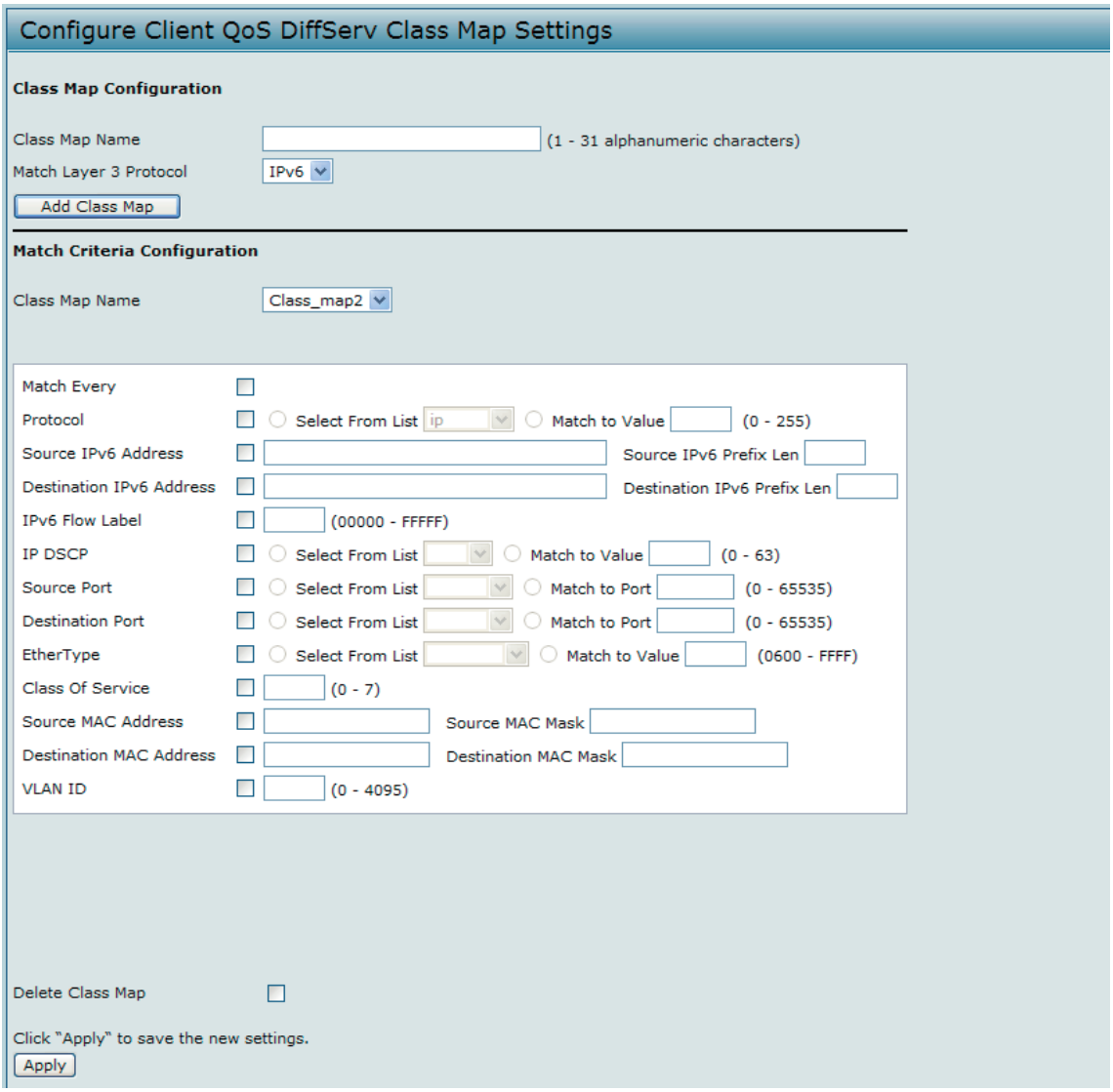


図 9-7　クライアント QoS DiffServ クラスマップ設定 画面 - IPv6

以下の項目を表示します。

項目	説明
Class Map Configuration	
Class Map Name	クラスマップ名（半角英数字 31 文字以内）を入力します。
Match Layer 3 Protocol	分類するパケットのタイプ（IPv4 または IPv6）を指定します。
Match Criteria Configuration	
Class Map Name	設定するクラス名を選択します。パケットをクラスに一致させるために本セクションの各項目を使用して設定します。クラスに評価基準として使用する各項目のチェックボックスを選択して、関連項目にデータを入力します。クラスに複数の一致する基準を持つことができます。 注意　利用可能な照合基準の欄は、クラスマップが IPv4 または IPv6 クラスマップかどうかによって異なります。
Match Every	照合条件が L3 パケット内のすべてのパラメータに一致するためには、これを選択します。すべての L3 パケットが Match Every の照合条件に一致します。

項目	説明
Protocol	「Protocol」欄を選択して、IPv4 パケットの IP Protocol フィールドの値または IPv6 パケットの Next Header フィールドに基づいて L3 または L4 プロトコルの一致条件を使用します。本欄を選択した場合、キーワードで照合するプロトコルを選択するか、またはプロトコル ID に入力します。 • Select From List リストからの以下のプロトコルの 1 つを選択します。 - ip - icmp - ipv6 - icmpv6 - igmp - tcp - udp • Match to Value 名前で表示されないプロトコルを照合するためには、プロトコル ID を入力します。プロトコル ID は、IANA によって割り当てられた基準値です。範囲は 0-255 の数値です。
IPv4 Class Maps	
Source IP Address	本欄を選択するとパケットの送信元ポートの IP アドレスがここで示すアドレスに一致する必要があります。適切な欄に IP アドレスを入力して、この基準を適用します。
Source IP Mask	送信元 IP アドレスを指定します。DiffServ のマスクは、パケットコンテンツとの照合に使用する送信先 IP アドレスの部分を指定する「.」（ドット）で区切った 10 進数形式のネットワーク型ビットマスクです。「255.255.255.255」の DiffServ マスクは、すべてのビットが重要で、「0.0.0.0」のマスクは、どのビットも重要でないことを示します。逆の場合は ACL ワイルドカードマスクに一致します。例えば、シングルホストアドレスに基準を一致させる場合は、「255.255.255.255」マスクを使用します。24 ビットのサブネット（例 :192.168.10.0/24）に基準を一致させる時は、「255.255.255.0」のマスクを使用します。
Destination IP Address	本欄を選択するとパケットの送信先 IP アドレスがここで示すアドレスに一致する必要があります。適切な欄に IP アドレスを入力して、この基準を適用します。
Destination IP Mask	送信先 IP アドレスマスクを入力します。DiffServ のマスクは、パケットコンテンツとの照合に使用する送信先 IP アドレスの部分を指定する「.」（ドット）で区切った 10 進数形式のネットワーク型ビットマスクです。「255.255.255.255」の DiffServ マスクは、すべてのビットが重要で、「0.0.0.0」のマスクは、どのビットも重要でないことを示します。逆の場合は ACL ワイルドカードマスクに一致します。例えば、シングルホストアドレスに基準を一致させる場合は、「255.255.255.255」マスクを使用します。24 ビットのサブネット（例 :192.168.10.0/24）に基準を一致させる時は、「255.255.255.0」のマスクを使用します。
IPv6 Class Maps	
Source IPv6 Address	本欄を選択するとパケットの送信元ポートの IPv6 アドレスがここで示すアドレスに一致する必要があります。適切な欄に IPv6 アドレスを入力して、この基準を適用します。
Source IPv6 Prefix Length	送信元 IPv6 アドレスのプレフィックス長を入力します。
Destination IPv6 Address	本欄を選択するとパケットの送信先 IPv6 アドレスがここで示すアドレスに一致する必要があります。適切な欄に IPv6 アドレスを入力して、この基準を適用します。
Destination IPv6 Prefix Length	送信先 IPv6 アドレスのプレフィックス長を入力します。
IPv6 Flow Label	IPv6 のフローラベルを 0000-FFFFF の範囲で指定します。
IP DSCP	To use IP DSCP as a match criteria, select the check box and select a DSCP value keyword or enter a DSCP. Select from List Select from a list of DSCP types. Match to Value Enter a DSCP Value to match (0 – 63).

項目	説明
IPv4 and IPv6 Class Maps	
Source Port	ルールの一致条件に送信元ポートを含める場合に選択します。送信元ポートはデータグラムヘッダで識別します。ポート名を指定するか、またはポート番号を入力します。 • Select From List 一致させる送信元ポートに関連するキーワードを選択します。 - ftp - ftpdata - http - smtp - snmp - telnet - tftp - www 各キーワードは相当するポート番号に変換されます。 • Match to Port データグラムヘッダで識別される送信元ポートに一致させる IANA ポート番号を入力します。ポート範囲は 0-65535 で、以下の 3 つの異なるポートタイプを含みます。 - 0-1023 - 通常のポート - 1024-49151 - 登録されたポート - 49152-65535 - ダイナミックおよび / またはプライベートポート
Destination Port	ルールの一致条件に送信先ポートを含める場合に選択します。送信先ポートはデータグラムヘッダで識別します。ポート名を指定するか、またはポート番号を入力します。 • Select From List 一致させる送信先ポートに関連するキーワードを選択します。 - ftp - ftpdata - http - smtp - snmp - telnet - tftp - www 各キーワードは相当するポート番号に変換されます。 • Match to Port データグラムヘッダで識別される送信先ポートに一致させる IANA ポート番号を入力します。ポート範囲は 0-65535 で、以下の 3 つの異なるポートタイプを含みます。 - 0-1023 : 通常のポート - 1024-49151 : 登録されたポート - 49152-65535 : ダイナミックおよび / またはプライベートポート
EtherType	この欄を選択すると、イーサネットフレームのヘッダ内の値と照合基準を比較します。EtherType のキーワードを選択するか、または EtherType 値を入力して、照合基準を指定します。 • Select from List Select 以下のプロトコルタイプの 1 つを選択します。 - appletalk - arp - ipv4 - ipv6 - ipx - netbios - pppoe • Match to Value パケットが照合されるカスタムプロトコル識別子を入力します。値は 0600-FFFF の範囲の 4 桁の 16 進数です。
Class Of Service	本欄を選択し、パケットと照合する CoS 802.1p ユーザ優先度値を入力します。値の範囲は 0-7 です。
Source MAC Address	本欄を選択し、Ethernet フレームと比較する送信元 MAC アドレスマスクを入力します。
Source MAC Mask	Ethernet フレームと比較する送信元 MAC のビット位置を指定する送信元 MAC アドレスマスクを入力します。
Destination MAC Address	本欄を選択し、Ethernet フレームと比較する送信先 MAC アドレスマスクを入力します。
Destination MAC Mask	Ethernet フレームと比較する送信先 MAC のビット位置を比較する送信先 MAC アドレスマスクを入力します。
VLAN ID	本欄を選択し、パケットと比較する VLAN ID を入力します。VLAN ID の範囲は 0-4095 です。
IPv4 Class Maps	

項目	説明
Service Type	クラス基準との照合に利用する 1 つのサービスタイプを指定します。
IP DSCP	一致基準として IP DSCP を使用するためには、チェックボックスを選択し、DSCP 値のキーワードを選択するか、または DSCP を入力します。 • Select from List - DSCP タイプ（af11-12、af21-23、af31-33、af41-43、cs0-7、ef）を選択します。 • Match to Value - 照合する DSCP 値（0-63）を入力します。
IP Precedence	本欄を選択すると、パケットの「IP Precedence」値をクラス基準の IP Precedence 値と照合します。IP Precedence 範囲は 0-7 です。
IP TOS Bits	一致基準として使用するパケットの IP ヘッダのサービスタイプのビット値を入力します。TOS ビット値の範囲は 00-FF です。上位 3 ビットは IP 優先度値を表します。上位 6 ビットは IP Differentiated Services Code Point（DSCP）値を表します。
IP TOS Mask	IP TOS マスク値を入力し、パケットのヘッダ内にあり、本ルールで入力した TOS と照合される TOS フィールドとのブーリアン型論理和を実行します。パケットの IP ヘッダ内の TOS フィールドからの指定されたビット（Precedence/Type of Service）を本ルールで入力した TOS と比較するために TOS マスクを使用することができます。（00-FF）。
Delete Class Map	チェックして、「Class Map Name」メニューで選択したクラスマップを削除します。既にポリシーに割り当てられている場合、クラスマップは削除できません。

クラスマップの削除

「Class Map Name」で削除するエントリを選択後、「Delete Class Map」オプションをチェックして「Apply」ボタンをクリックします。

Polcy Map（Diffserv ポリシーマップの作成）

DiffServ ポリシーを作成し、クラスのコレクションを 1 つ以上のポリシーステートメントと関連付けます。

パケットは、定義した基準に基づいて分類されて、処理されます。分類の基準は、**Client QoS > Class Map** 画面でクラスごとに定義されます。その処理は、以下のポリシーマップ設定画面でポリシーの属性によって定義されます。ポリシーの属性はクラスごとにインスタンスベースで定義し、これらの属性は一致する場合に適用されます。ポリシーには、複数のクラスを含めることができます。ポリシーがアクティブな場合は、パケットがどのクラスに一致するかによって、アクションを行います。

パケット処理は、パケットに対してクラスの基準に一致するかどうかをテストすることで開始します。そのポリシーで一致するクラスが見つかると、ポリシーがパケットに適用されます。

DiffServ ポリシーの作成手順

1. **Client QoS > Policy Map** の順にメニューをクリックし、以下の画面を表示します。

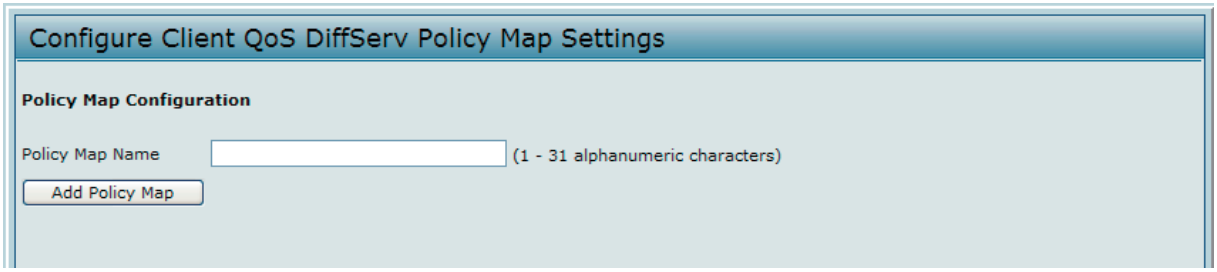

Configure Client QoS DiffServ Policy Map Settings
Policy Map Configuration
Policy Map Name
(1 - 31 alphanumeric characters)
Add Policy Map

図 9-8　クライアント QoS DiffServ ポリシーマップ設定 画面

2. 「Policy Map Name」にポリシー名を入力後、「Add Policy Map」ボタンをクリックして、以下の画面を表示します。

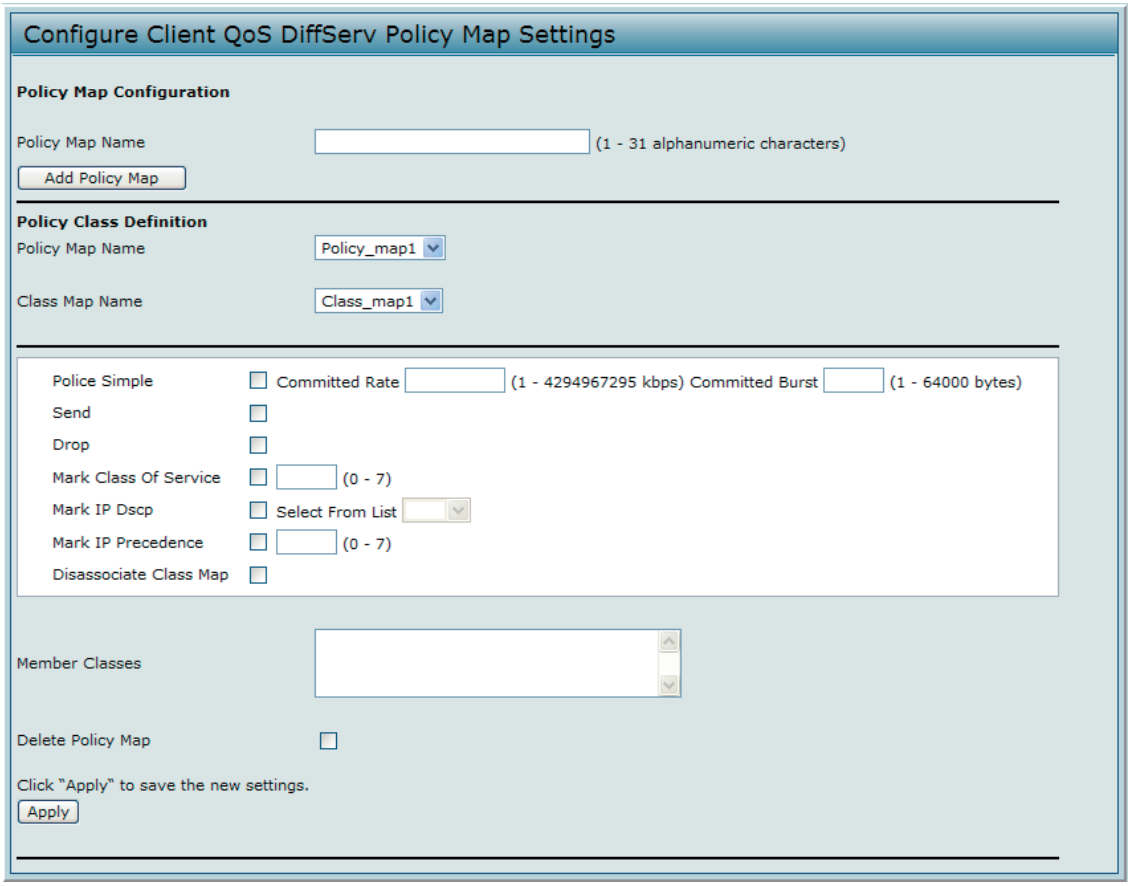


図 9-9　クライアント QoS DiffServ ポリシーマップ設定 画面 - ポリシーマップ追加

画面には以下の項目があります。

項目	説明
Policy Map Configuration	
Policy Map Name	追加するポリシーマップ名を入力します。半角英数字 31 以内で指定します。
Policy Class Definition	
Policy Map Name	メンバクラスに関連付けるポリシーを選択します。
Class Map Name	このポリシー名に関連付けるメンバクラスを選択します。
詳細設定	
Policy Simple	クラスにトラフィックポリシングスタイルを設定します。ポリシングスタイルのシンプルな形式では、単一のデータレートとバーストサイズを使用します。適合と違反の 2 つの結果がもたらされます。
Committed Rate	トラフィックが適合する必要のあるコミット速度（1 - 4294967295 Kbps）を入力します。
Committed Burst	トラフィックが適合する必要のあるコミットバーストサイズ（1- 64000Kbps）を入力します。
Send	クラスマップ基準が満たされる場合に関連トラフィックストリームのすべてのパケットが転送されることを指定します。
Drop	クラスマップ基準が満たされる場合に関連トラフィックストリームのすべてのパケットが破棄されることを指定します。
Mark Class Of Service	本欄を選択すると、802.1p ヘッダの優先度フィールドに指定したサービスクラスに関連するトラフィックストリームに対するパケットのすべてにマークを付けます。パケットがまだこのヘッダを持っていない場合、1 つ挿入されます。CoS 値は、0-7 の整数です。
Mark IP Dscp	本欄を選択すると、リストから選択した、または入力した IP DSCP 値に関連するトラフィックストリームに対するパケットのすべてをマークします。 • Select From List - DSCP タイプ（af11-12、af21-23、af31-33、af41-43、cs0-7、ef）をリストから選択します。
Mark IP Precedence	本欄を選択すると、指定した IP Precedence 値に関連するトラフィックストリームに対するパケットのすべてをマークします。IP Precedence 値は、0-7 の整数です。
Disassociate Class Map	本オプションを選択し、「Apply」ボタンをクリックして「Policy Map Name」で選択したポリシーから「Class Map Name」で選択したクラスを削除します。
Member Classes	現在定義されているすべての DiffServ クラスを選択されたポリシーのメンバとして表示します。ポリシーと関連するクラスがない場合、本欄は空白です。
Delete Policy Map	本欄を選択し、「Policy Map Name」で選択したポリシーマップを削除します。

ポリシーマップの削除

「Delete Policy Map」オプションを選択し、「Apply」ボタンをクリックします。

Client QoS Status（クライアント QoS ステータス）

現在アクセスポイント接続している各クライアントに適用されるクライアント QoS 設定を表示します。

接続クライアントに関する QoS 設定を参照するためには、**Client QoS > Client QoS Status** の順にメニューをクリックし、以下の画面を表示します。

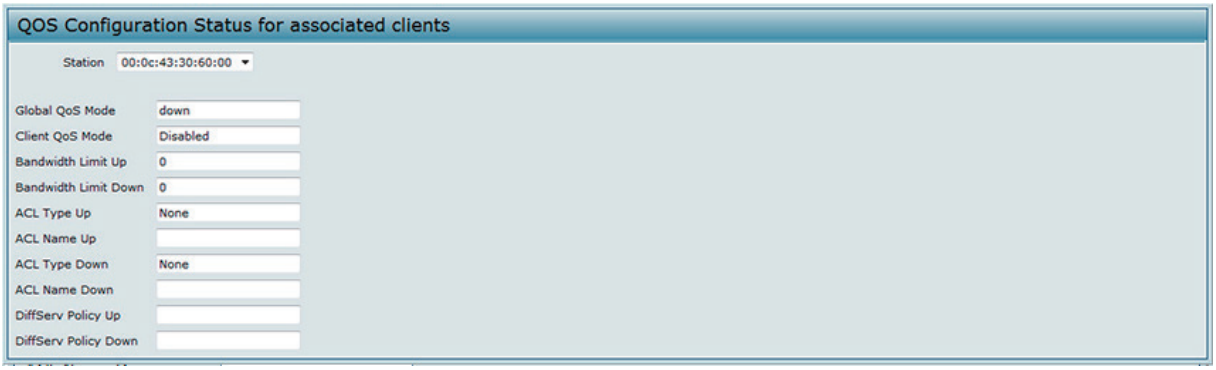


図 9-10　接続クライアントの QoS 設定ステータス 画面

画面には次の項目があります。

項目	説明
Station	現在アクセスポイントに接続している各クライアントの MAC アドレスが含まれます。そのクライアントに適用されている QoS 設定を参照するためには、リストから MAC アドレスを選択します。
Global QoS Mode	選択クライアントの QoS モードが有効または無効であるかを表示します。 **注意** QoS モードがクライアントに有効とするためには、アクセスポイントでそれをグローバルに有効にし、クライアントが接続する VAP でも有効にします。**Client QoS > VAP QoS Parameters** メニューを使用して、「QoS Global Admin Mode」と VAP ごとの「QoS Mode」を有効にします。
Client QoS Mode	選択クライアントの QoS モードが有効または無効であるかを表示します。 **注意** QoS モードがクライアントに有効とするためには、アクセスポイントでそれをグローバルに有効にし、クライアントが接続する VAP でも有効にします。**Client QoS > VAP QoS Parameters** メニューを使用して、「QoS Global Admin Mode」と VAP ごとの「QoS Mode」を有効にします。
Bandwidth Limit Down	クライアントがアクセスポイントからトラフィックを受信する最大レート（bps）を表示します。 有効範囲は 0-4294967295（bps）です。
Bandwidth Limit Up	クライアントがアクセスポイントにトラフィックを送信する最大レート（bps）を表示します。有効範囲は 0-4294967295（bps）です。
ACL Type Down	外向き（アクセスポイントからクライアント）トラフィックに適用される ACL のタイプは示します。これは、IPv4 だけです。ACL は ACL ルールへの一致があるかどうか IPv4 パケットを調べます。
ACL Name Down	外向きトラフィックに適用する ACL 名を表示します。パケットまたはフレームが外向きのインタフェースに変更されると、ACL ルールが照合のためにチェックされます。パケットまたはフレームは、許可された場合には送信され、拒否された場合には廃棄されます。
ACL Type Up	内向き（クライアントからアクセスポイント）トラフィックに適用される ACL のタイプは示します。これは、IPv4 だけです。ACL は ACL ルールへの一致があるかどうか IPv4 パケットを調べます。
ACL Name Up	内向きにアクセスポイントから送信されるトラフィックに適用する ACL 名を表示します。パケットまたはフレームをアクセスポイントが受信すると、ACL ルールが照合のためにチェックされます。パケットまたはフレームは、許可された場合には処理され、拒否された場合には廃棄されます。
DiffServ Policy Down	外向き（アクセスポイントからクライアント）にアクセスポイントから送信されるトラフィックに適用する DiffServ ポリシー名を表示します。
DiffServ Policy Up	内向き（クライアントからアクセスポイント）に送信されるトラフィックに適用する DiffServ ポリシー名を表示します。

Configuring RADIUS-Assigned Client QoS Parameters（RADIUS クライアント QoS パラメータ）

VAP が「WPA Enterprise」セキュリティを設定している場合、RADIUS サーバのクライアントデータベース内にクライアント QoS 情報を含むことが可能です。クライアントが認証に成功した時、RADIUS サーバは帯域限度を含み、特定の無線クライアントに適用するための ACL と DiffServ ポリシーを識別することが可能です。RADIUS クライアントデータベースに参照される ACL と DiffServ ポリシーは無線クライアントに適用するために、必ず ACL 名と AP で設定された DiffServ ポリシー に合致する必要があります。

次の表はクライアントの RADIUS サーバエントリに含むことのできる QoS 属性にについて説明します。無線クライアントが「WPA Enterprise」を使用した認証に成功した場合、クライアントのために存在する各 QoS RADIUS 属性はプロセスで AP に送信されます。この属性はオプションで、クライアントエントリには必要ありません。もし属性がない場合は AP の「Client QoS」設定を使用します。

RADIUS Attribute	ID	Description	Type/Range
Vendor-Specific (26), WISPr-Bandwidth-Max-Down	14122,8	クライアントの最大受信速度（b/s）。クライアントがネットワークからデータを受信できる帯域を制限します。ゼロでないの場合、AP で使用している 64Kbps に一番近い値に繰り下げられます。(64 Kbps が最小) 属性が 0 の場合、帯域の限度はこの方向ではクライアントに強制しません。	種類：integer 32 ビット符号なし整数値 (0-4294967295)
Vendor-Specific (26), WISPr-Bandwidth-Max-Up	14122,7	クライアントの最大受信速度（b/s）。クライアントがネットワークからデータを受信できる帯域を制限します。ゼロでないの場合、AP で使用している 64Kbps に一番近い値に繰り下げられます。(64 Kbps が最小) 属性が 0 の場合、帯域の限度はこの方向ではクライアントに強制しません。	種類：integer 32 ビット符号なし整数値 (0-4294967295)
Vendor-Specific (26), LVL7-Wireless -Client- ACL-Dn	6132,120	アウトバウンド（ダウン）の 802.1X 認証無線クライアントトラフィックに適用する ACL 識別。AP に存在しない ACL に属性を参照する場合、クライアントへの全てのパケットは ACL が定義されるまで廃棄されます。	種類：string 5-36 半角英字（Null-terminated 無し） 文字列は以下の通り、「type:name」形式になります。: • type = ACL タイプ識別子：IPV4、IPV6、MAC •「：」は区切り文字として必要です。 • name= 英数字 (1-31 文字) で ACL 番号 (IPv4) または名称 (IPv6、MAC) を示します。
Vendor-Specific (26), LVL7-Wireless-Client-ACL-Up	6132,121	アウトバウンド（アップ）の 802.1X 認証無線クライアントトラフィックに適用する ACL 識別。AP に存在しない ACL に属性を参照する場合、クライアントへの全てのパケットは ACL が定義されるまで廃棄されます。	種類：string 5-36 半角英字（Null-terminated 無し） 文字列は以下の通り、「type:name」形式になります。: • type = ACL タイプ識別子：IPV4、IPV6、MAC •「：」は区切り文字として必要です。 • name= 英数字 (1-31 文字) で ACL 番号 (IPv4) または名称 (IPv6、MAC) を示します。
Vendor-Specific (26), LVL7-Wireless-Client-Policy-Dn	6132,122	アウトバウンド（ダウン）の 802.1X 認証無線クライアントトラフィックに適用する DiffServ ポリシー名。AP に存在しない ACL に属性を参照する場合、クライアントへの全てのパケットは DiffServ ポリシーが定義されるまで廃棄されます。	種類：string 1-31 半角英字（Null-terminated されていない）
Vendor-Specific (26), LVL7-Wireless-Client-Policy-Up	6132,123	アウトバウンド（アップ）の 802.1X 認証無線クライアントトラフィックに適用する DiffServ ポリシー名。AP に存在しない ACL に属性を参照する場合、クライアントへの全てのパケットは DiffServ ポリシーが定義されるまで廃棄されます。	種類：string 1-31 半角英字（Null-terminated されていない）

第 10 章　Cluster（アクセスポイントのクラスタリング）

本製品は、AP クラスタをサポートしています。クラスタは、シングルポイントの管理を供給して、個別の無線デバイスのシリーズをむしろ単一のエンティティとして無線ネットワークを参照、配置、設定および保証させることができます。

設定項目	説明	参照ページ
Access Points（クラスタによるアクセスポイントの管理）	クラスタメンバの参照と設定を行います。	129 ページ
Sessions（クラスタセッションの管理）	クラスタ内のアクセスポイントに接続するクライアントステーションの情報を表示します。	132 ページ
Channel Management（チャンネルの管理）	クラスタメンバにチャンネル割り当ての設定、または参照を行います。	133 ページ
Wireless Neighborhood（無線近接デバイス情報の参照）	Neighbor アクセスポイントの無線インタフェースの統計情報と識別情報を表示します。	136 ページ

本章におけるこれらの機能の設定画面は、Web ユーザインタフェースのメインメニューから「Cluster」をクリックして表示します。

Access Points（クラスタによるアクセスポイントの管理）

AP クラスタはネットワークの同じサブネットにあるアクセスポイントのダイナミックなコンフィグレーションに対応するグループです。各クラスタは最大 16 個のメンバを持つことができます。1 つの無線ネットワークあたり 1 個のクラスタだけがサポートされていますが、ネットワークサブネットは複数のクラスタを持つことができます。クラスタは VAP 設定や QoS キューパラメータなどの様々な設定情報を共有できます。

以下の条件が満たされる場合、2 つのアクセスポイント間でクラスタを形成できます。

- アクセスポイントは同じ無線モードを使用します。例えば、radio 1 は 802.11g を使用します。
- アクセスポイントは同じブリッジを使用したセグメントで接続されます。
- クラスタを接続するアクセスポイントは、同じクラスタ名を持っています。
- クラスタリングモードは両方のアクセスポイントで有効とします。

注意 2 つのアクセスポイントが同じクラスタに所属するためには、同じ無線インタフェース番号を持つ必要はありませんが、無線帯のサポート機能は同じである必要があります。

シングルおよびデュアル無線インタフェース搭載アクセスポイントのクラスタリング

クラスタは 2 つの無線インタフェースを持つアクセスポイントと 1 つの無線インタフェースを持つアクセスポイントを混在することができます。クラスタ内の single-radio（シングル無線周波数帯）アクセスポイントの設定を変更する場合、アクセスポイントはすべてのクラスタメンバの最初の無線周波数帯に変更を伝達します。クラスタ内のどのような dual-radio（デュアル無線周波数帯）アクセスポイントの設定は影響も受けません。

クラスタが single-radio アクセスポイントだけを含み、ここに dual-radio アクセスポイントが参加すると、dual-radio アクセスポイントの Radio 1 だけがクラスタコンフィグレーションに設定されます。Radio 1 がクラスタへの参加に対して優先されるため、アクセスポイントの Radio 2 は残ります。しかし、クラスタに少なくとも 1 つの dual-radio アクセスポイントが既にあると、クラスタに参加するアクセスポイントの 2 番目の無線インタフェースにクラスタ設定が行われます。

クラスタメンバの参照と設定

アクセスポイントのクラスタリングの開始または停止、クラスタメンバの参照、クラスタメンバのロケーションとクラスタ名の設定を行います。また、クラスタ内のアクセスポイントに関するコンフィグレーションとデータを表示します。

クラスタメンバに関する情報の参照と各メンバのロケーションとクラスタの設定を行うためには、**Cluster > Access Points** の順にメニューをクリックして以下の画面を表示します。

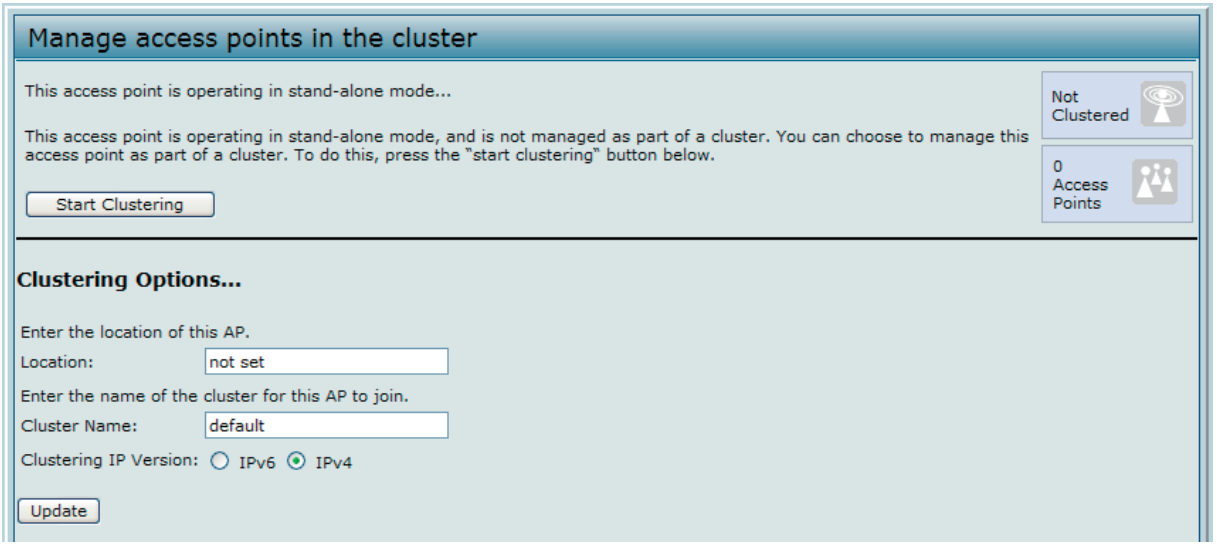


図 10-1　クラスタ内のアクセスポイントの管理 画面 - クラスタリングが無効

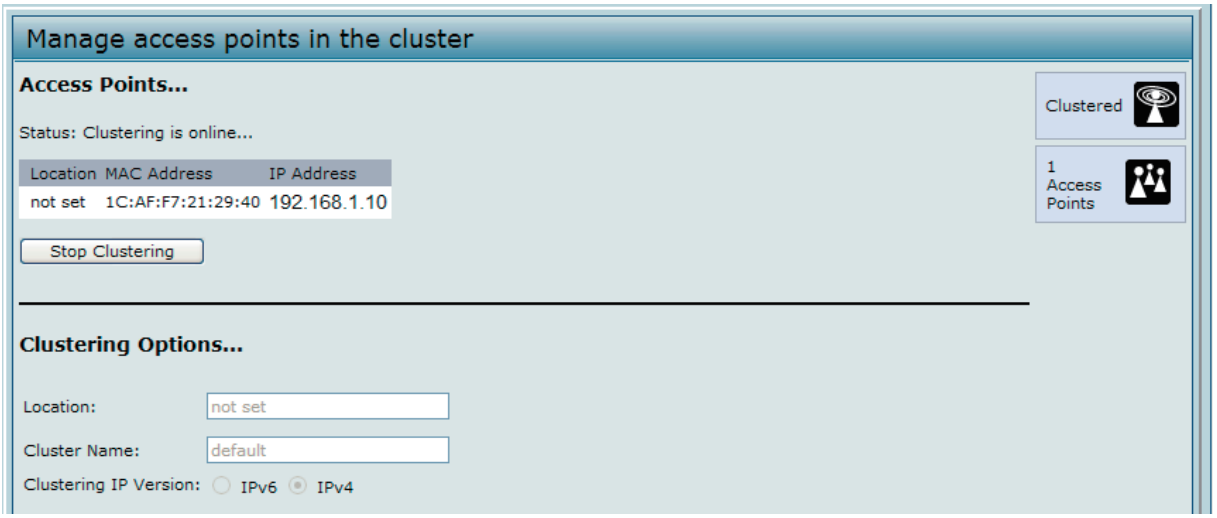


図 10-2　クラスタ内のアクセスポイントの管理 画面 - クラスタリングが有効

クラスタリングが現在アクセスポイントで無効である場合には、「Start Clustering」ボタンが表示されます。クラスタリングが有効である場合には、「Stop Clustering」ボタンが表示されます。クラスタリングがいつ無効にされるかというクラスタリングオプション情報を編集することができます。

以下の表では「Access Points」画面で利用可能な設定およびステータス情報について説明します。

項目	説明
Status	本欄が表示されると、アクセスポイントはクラスタリングは有効です。クラスタリングが有効でない場合、アクセスポイントはスタンドアロンモードで動作している旨のみ表示されます。アクセスポイントでクラスタリングを無効にするためには、「Stop Clustering」ボタンをクリックします。
Location	アクセスポイントが物理的に位置している場所に関する説明。
MAC Address	アクセスポイントの MAC アドレス。ここに示されるアドレスは、ブリッジ (br0) の MAC アドレスです。これは、アクセスポイントが外部的に他のネットワークに知られているアドレスです。
IP Address	アクセスポイントの IP アドレスを指定します。 各 IP アドレスはそのアクセスポイントの管理 Web 画面にリンクしています。そのリンクを使用して、特定のアクセスポイントの管理 Web 画面に遷移します。これは、クラスタメンバがクラスタ設定の変更をピックアップしていることを確認するため、特定のアクセスポイントにおける詳細設定を行うため、またはスタンドアロンアクセスポイントをクラスタモードに切り替えるために、特定のアクセスポイントのデータを参照する場合に有効です。

以下の表は、個別のメンバに設定するクラスタ情報について説明しています。クラスタリングが有効な場合、クラスタリングオプションは読み取りだけできます。クラスタリングオプションを設定するためには、「Stop Clustering」ボタンをクリックしてクラスタリングを停止します。

項目	説明
Location	アクセスポイントが物理的に位置している場所に関する説明を入力します。
Cluster Name	アクセスポイントが接続するクラスタ名前を入力します。クラスタ名はクラスタ内の他のアクセスポイントには送信されません。クラスタのメンバである各アクセスポイントには同じクラスタ名を設定する必要があります。クラスタ名はネットワーク内の各クラスタごとに固有である必要があります。
Clustering IP Version	クラスタ内のアクセスポイントが相互に通信するために使用する IP バージョン（IPv6 または IPv4）を指定します。

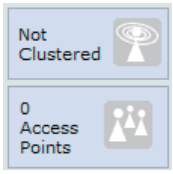
クラスタからアクセスポイントを削除する

クラスタからアクセスポイントを削除するためには、以下の手順を行いいます。

1. クラスタリングしているアクセスポイントの管理 Web マネージャを表示します。

2. **Cluster > Access Points** メニューをクリックします。

3. 「Stop Clustering」ボタンをクリックします。
   本変更により、画面は更新されて現在のステータスが表示されます。アクセスポイントの「Status」の下に反映されます。アクセスポイントは（クラスタの代わりに）スタンドアロンモードとして表示されます。ステータスアイコンは以下の通り「Not Clustered」となります。



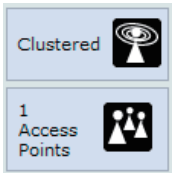
クラスタにアクセスポイントを追加する

現在、スタンドアロンモードであるアクセスポイントをクラスタに追加するためには、以下の手順を行います。

1. スタンドアロンモードのアクセスポイントの管理 Web マネージャを表示します。

2. スタンドアロンモードのアクセスポイントで **Cluster > Access Points タブ**の順にメニューをクリックします。

3. 「Start Clustering」ボタンをクリックします。
   アクセスポイントはクラスタメンバになります。**Cluster > Access Points** の「Status」は、「Not Clustered」の代わりにクラスタを表示します。ステータスアイコンは以下の通り「Clustered」となります。



特定アクセスポイントの設定情報への移動

一般に、統合アクセスポイントは、クラスタリングしているアクセスポイントの中央管理のために設計されています。クラスタ内のアクセスポイントにより、クラスタ内のすべてのアクセスポイントが同じコンフィグレーションを反映します。この場合、管理のために実際にどのアクセスポイントに接続するかは重要ではありません。

しかし、特定のアクセスポイントに関する情報を参照、または管理する場合、いくつかの状況が考えられます。例えば、アクセスポイントのクライアント接続またはイベントなどのステータス情報のチェックを行う場合があります。この時、図 10-2 にある IP アドレスのリンクをクリックすることによって、各アクセスポイントの管理 Web インタフェースに移動することができます。

すべてのクラスタリングしているアクセスポイントは **Cluster > Access Points** 画面に表示されます。クラスタリングしているアクセスポイントへ移動するためには、リストに示される特定のクラスタメンバの IP アドレスをクリックします。

URL に IP アドレス使用してアクセスポイントに移動する

以下の形式で Web ブラウザのアドレスにそのアクセスポイントの IP アドレスを入力することで特定のアクセスポイントの管理 Web 画面にリンクできます。

http:// アクセスポイントの IP アドレス

「アクセスポイントの IP アドレス」は、モニタリングまたは設定する特定のアクセスポイントのアドレスです。

Sessions（クラスタセッションの管理）

クラスタ内のアクセスポイントに接続するクライアントステーションの情報を表示します。各クライアントは、現在接続するアクセスポイント（ロケーション）と共に MAC アドレスで識別されます。

クラスタに関連しているセッションを管理します。はじめに、**Cluster > Access Points** でクラスタを開始する必要があります。

Cluster > Sessions の順にメニューをクリックし、以下の画面を表示します。

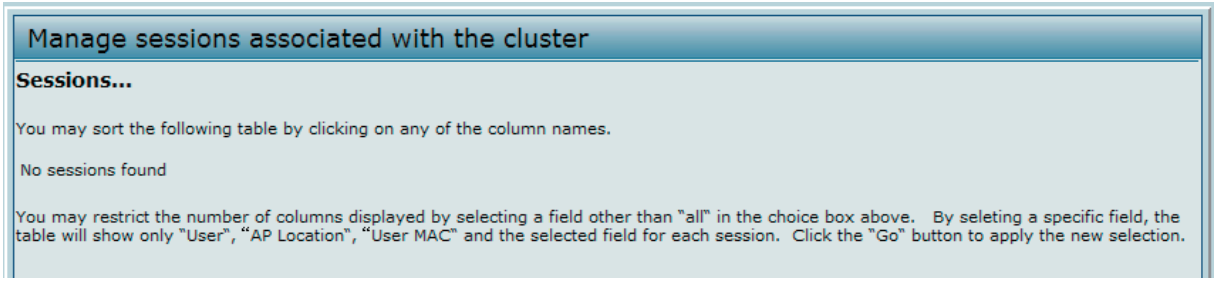


図 10-3　クラスタに接続するセッションの管理 画面 - セッションなし

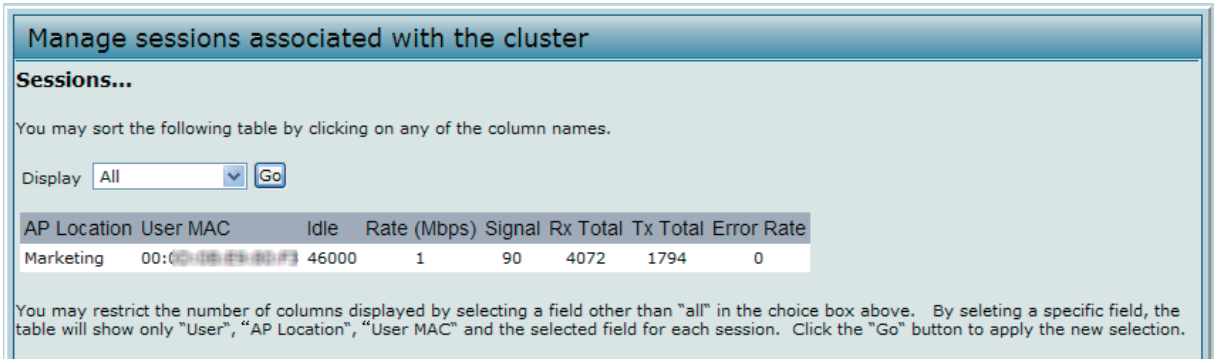


図 10-4　クラスタに接続するセッションの管理 画面 - セッションあり

クライアントセッションの特定の統計情報を参照するためには、「Display」プルダウンメニューから表示する項目を選択し、「Go」ボタンをクリックします。アイドルタイム、データレート、信号強度などの情報を参照できます。これらのすべてが以下の表で詳細に説明されます。

この場面のセッションは、固有の MAC アドレスを持つクライアントデバイス（Station）のユーザが無線ネットワークとの接続を維持する期間です。クライアントがネットワークにログインするとセッションが開始し、クライアントが意識的にログアウトする場合、またはその他の理由で接続を失った場合にセッションは終了します。

注意　セッションは、アソシエーションとは異なり、特定のアクセスポイントへのクライアント接続について説明しています。クライアントネットワーク接続は、同じセッション内のコンテキスト内で 1 つのクラスタリングしているアクセスポイントから別のものに移行することができます。クライアントステーションは、アクセスポイント間をローミングして、セッションを維持します。

表示されるセッション情報に関する詳細は、以下の表で説明します。

項目	説明
Display	表示する統計情報を All、Idle Time、Data Rate、Signal、Receive Total、Transmit Total、Error Rate から選択します。
AP Location	これは、**Basic Settings** メニューで指定したロケーションの説明から取得します。
User MAC	無線クライアントデバイスの MAC アドレスを示します。
Idle	このステーションの無効のままであった時間に示します。データの受信、または送信していない場合、ステーションがアイドル状態であると見なされます。
Rate (Mbps)	このアクセスポイントが指定クライアントにデータを送信する速度。データ送信速度は Mbit/ 秒で示されます。この値は、アクセスポイントで使用中のモードに通知されている速度設定の範囲内に下げるべきです。例えば、802.11a では 6-54Mbps とします。
Signal	クライアントがアクセスポイントから受信する無線周波（RF）信号の強さを示します。これに使用される方法は、Received Signal Strength Indication（RSSI）として知られている値（0-100）です。RSSI はクライアントステーションのネットワークインタフェースカード（NIC）に実装されたメカニズムで決定されます。
Rx Total	現在のセッション間にクライアントが受信した総パケット数を示します。
Tx Total	このセッションでクライアントに送信した総パケット数を示します。
Error Rate	このアクセスポイントにおいて伝送の間に破棄された時間フレームの割合を示します。

セッション情報のソート

テーブルに示される情報を特定の指示でソートするためには、並べ替える欄のラベルをクリックします。例えば、信号強度で並べたテーブルの行を参照する場合、「Signal」欄のラベルをクリックします。エントリは信号強度によってソートされます。

Channel Management（チャンネルの管理）

チャンネル管理が有効な場合、本製品は自動的にクラスタリングしているアクセスポイントが使用する無線チャンネルを割り当てます。自動チャンネル割り当ては、相互干渉（または、クラスタの外側にある他のアクセスポイントとの混信）を抑制し、Wi-Fi 帯域幅を最大にすることで無線ネットワークの通信効率を維持するために役立ちます。

自動チャンネル割り当てを行うためには、チャンネル管理を開始する必要があります。新しいアクセスポイントの初期値は「Disabled」（無効）になっています。

指定間隔で、チャンネルマネージャがアクセスポイントにチャンネルの使用を割り当てて、クラスタ内の干渉レベルを測定します。重要なチャンネル妨害が検出されると、チャンネルマネージャは自動的に効率のよいアルゴリズム（または、自動化されたチャンネルプラン）に従って新しいチャンネルにアクセスポイントのいくつかまたはすべてを再度割り当てます。

クラスタリングしているアクセスポイントの過去、現在、および計画されたチャンネル割り当てを表示します。

クラスタメンバにチャンネル割り当ての設定、または参照を行うためには、**Cluster > Channel Management** の順にメニューをクリックし、以下の画面を表示します。

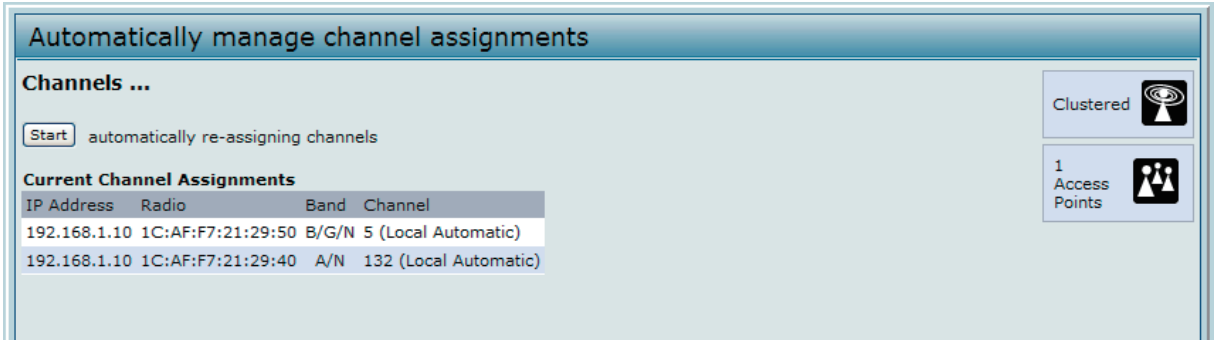


図 10-5　チャンネル割り当ての管理 画面 - 自動チャンネル割り当て無効

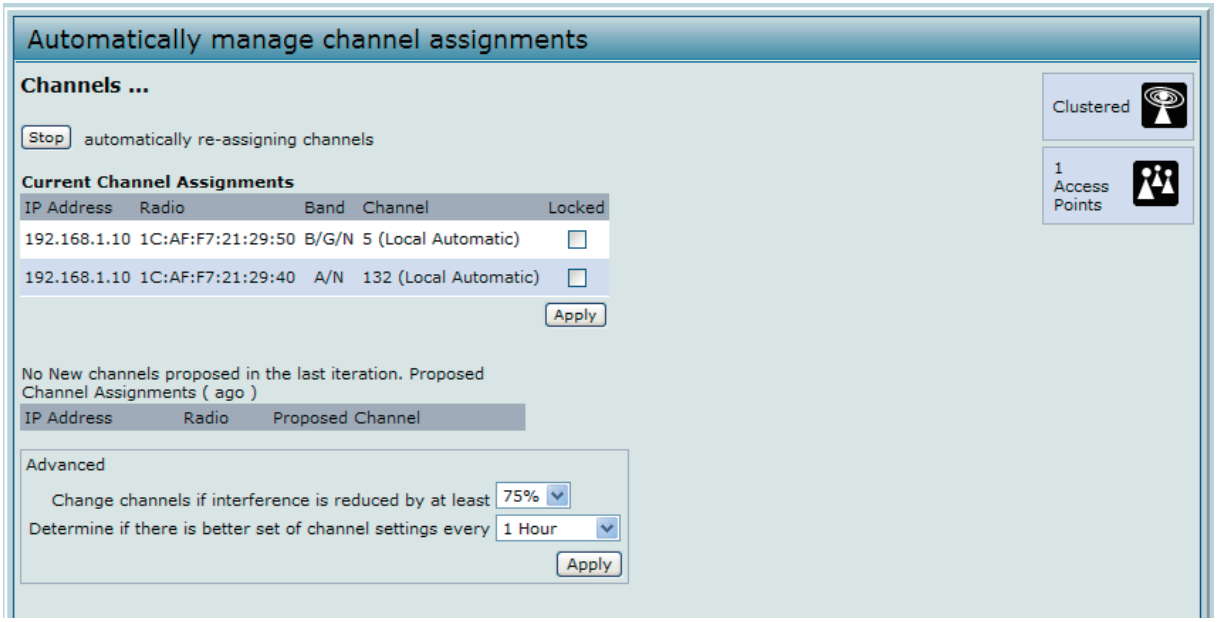


図 10-6　チャンネル割り当ての管理 画面 - 自動チャンネル割り当て有効

画面の「Advanced」セクションでは、チャンネルの再割り当てを始動する干渉を低減する可能性の変更、自動更新のスケジュールの変更、および割り当てに使用されるチャンネルセットの再設定を行うことができます。

自動チャンネル割り当ての開始と中止

初期値では、自動チャンネル割り当ては無効です。

注意 チャンネル管理は、クラスタを経由してすべてのアクセスポイントの無線チャンネルに同期させるデフォルトクラスタの動作を上書きします。チャンネル管理が有効にされると、無線チャンネルはクラスタ経由で他のアクセスポイントと同期しません。

自動チャンネル割り当ての再開

「Start」ボタンをクリックして、自動チャンネル割り当てを再開します。自動チャンネル割り当てが有効にされると、チャンネルマネージャは、定期的にクラスタリングされているアクセスポイントが使用する無線チャンネルを割り当てて、必要な場合、クラスタリングされているアクセスポイントのチャンネルの再割り当てを行い、（クラスタメンバまたはクラスタの外側にあるアクセスポイントとの）干渉を軽減します。

自動チャンネル割り当ての停止

「Stop」ボタンをクリックして、自動チャンネル割り当てを停止します。どのチャンネルの使用のためのマップもチャンネルの再割り当ては行われません。手動の更新だけがチャンネル割り当てに影響します。

注意 **Manage > Radio** 画面の「Channel」欄が「Auto」に設定されると、提案されたチャンネルの割り当ては実施されません。チャンネルをスタティックなチャンネルに設定する必要があります。

現在のチャンネル割り当ての参照とロックの設定

IP アドレスごとにクラスタ内の全アクセスポイントのリストを表示します。各アクセスポイントがブロードキャストする無線帯域（a/b/g/n）、各アクセスポイントが使用する現在のチャンネル、および別に再割り当てされないように現在の無線チャンネルにあるアクセスポイントをロックするオプションを表示します。

以下の表で現在のチャンネル割り当てに関する詳細を提供します。

項目	説明
IP Address	アクセスポイントの IP アドレスを指定します。
Radio	無線インタフェースの MAC アドレスを示します。
Band	アクセスポイントがブロードキャストを行っている無線インタフェースを示します。
Current	アクセスポイントが現在ブロードキャストを行っている無線チャンネルを示します。
Locked	チェックするとアクセスポイントを現在のチャンネルに残すように設定します。 アクセスポイントに選択される（有効な）場合、自動化されたチャンネル管理プランは最適化戦略の一部として異なるチャンネルにアクセスポイントを再割り当てしません。代わりにロックされたチャンネルを持つアクセスポイントがそのプランのための要求として要素に盛り込まれます。 「Apply」ボタンをクリックすると、ロックされたアクセスポイントが「Current Channel」と「Proposed Channel」欄に同じチャンネルを表示することがわかります。ロックされたアクセスポイントは、現在のチャンネルを保持します。

最後に提案された変更の設定を参照する

「Proposed Channel Assignments」は最後のチャンネルプランを表示します。プランは、IP アドレスごとにクラスタ内のすべてのアクセスポイントを示し、各アクセスポイントに対する現在のチャンネルと提案されたチャンネルを示します。ロックされたチャンネルは再割り当てされません。また、アクセスポイント間のチャンネル配布の最適化は、ロックされたアクセスポイントがそれらの現在のチャンネルに残る必要があるという事実を考慮に入れています。ロックされていないアクセスポイントは、プランの結果によっては、それらが以前に使用していたのものとは異なるチャンネルに割り当てられる可能性があります。

項目	説明
IP Address	アクセスポイントの IP アドレスを指定します。
Radio	アクセスポイントが現在ブロードキャストを行っている無線チャンネルを示します。
Proposed Channel	チャンネルプランが実行される場合、このアクセスポイントが再割り当てされる無線チャンネルを示します。

システムの詳細設定

詳細設定により、クラスタに対してチャンネルプランのカスタマイズとスケジューリングを行うことができます。（Advanced Settings を更新しないで）提供されるようなチャンネル管理を使用すると干渉を 25% 以上抑制できる場合、チャンネルは 1 時間に 1 回自動的に微調整されます。ネットワークが使用中でも、チャンネルは割り当てされます。適切なチャンネルセット（IEEE 802.11b/g を使用しているアクセスポイントには「b/g」、IEEE 802.11a を使用するアクセスポイントには「a」）が使用されます。

初期設定は、チャンネル管理を実行する必要がある多くのシナリオを満たすように設計されています。

チャンネルの再割り当てを始動する干渉を低減する可能性の変更、自動更新のスケジュールの変更、および割り当てに使用されるチャンネルセットの再設定を行います。「Advanced」セクションで表示する欄がないと、切り替えボタンをクリックして、チャンネルプランアルゴリズムのタイミングと詳細を変更する設定を表示します。

項目	説明
Change channels if interference is reduced by at least	提案されたプランが適用されるために実現するべき干渉の低減の割合（最小値）を指定します。初期値は 75% です。プルダウンメニューを使用して、5-75% の範囲で割合を選択します。本設定では、ネットワークは効率よく最低限の利得のために絶えず中断させることがないようにチャンネルの再割り当てのためのゲート要素を設定できます。例えばチャンネル干渉を 75% 抑制し、提案されたチャンネル割り当てが干渉を 30% 抑制しただけであると、チャンネルは再割り当てされません。しかし、チャンネル干渉の最低利得を 25% にリセットして、「Apply」ボタンをクリックすると、提案されたチャンネルプランは、実行されて、必要に応じてチャンネルが再割り当てされます。
Determine if there is better set of channels every	プルダウンメニューを使用して、自動更新のスケジュールを選択します。30 Minutes（30 分）から 6 Months（6 ヶ月）までさまざまな間隔を提供します。初期値は 1 Hour（1 時間）です。チャンネルの再割り当てとその結果生じるチャンネルプランが毎時間適用されます。

「Advanced」設定の「Apply」をクリックして、これらの設定を適用します。「Advanced」設定は、それらが適用されていると作用し、自動チャンネル管理がどう実行されるかに影響します。

Wireless Neighborhood（無線近接デバイス情報の参照）

クラスタ内の全メンバの適用範囲で無線インタフェースごとに最大 20 個のアクセスポイントを表示し、どのアクセスポイントがどのクラスタメンバの適用範囲にあるを表示します。また、クラスタメンバとクラスタメンバでないものを区別します。

注意 ここでは、無線インタフェースごとに最大 20 個のアクセスポイントを表示します。指定のクラスタアクセスポイントで検出されたアクセスポイントのすべてを参照するためには、そのクラスタメンバの Web インタフェースに移動し、**Status > Neighboring Access Points** 画面を表示します。

各 Neighbor アクセスポイントに対して無線インタフェースの統計情報（信号強度、チャンネル、ビーコン間隔）と共に識別情報（SSID、ネットワーク名、IP アドレス、MAC アドレス）を表示します。アクセスポイントをクリックし、現在選択しているアクセスポイントの無線帯域の範囲内にあるアクセスポイントに関する追加の統計情報を取得します。

以下の項目を表示します。

- 無線ドメイン内で予期しない（不正な）アクセスポイントを検出して、関連するリスクを制限するためにアクションをとれるような場所におきます。
- 予測される適用範囲を検証します。アクセスポイントが他のアクセスポイントからの信号強度の大きさを目に見えるもので評価することによって、配置が計画している目標を達成することを確認することができます。
- 故障を検出します。適用範囲パターン内の予期しない変更は、カラーコード化テーブルにより一目で明白となります。

Cluster > Wireless Neighborhood の順にメニューをクリックし、以下の画面を表示します。

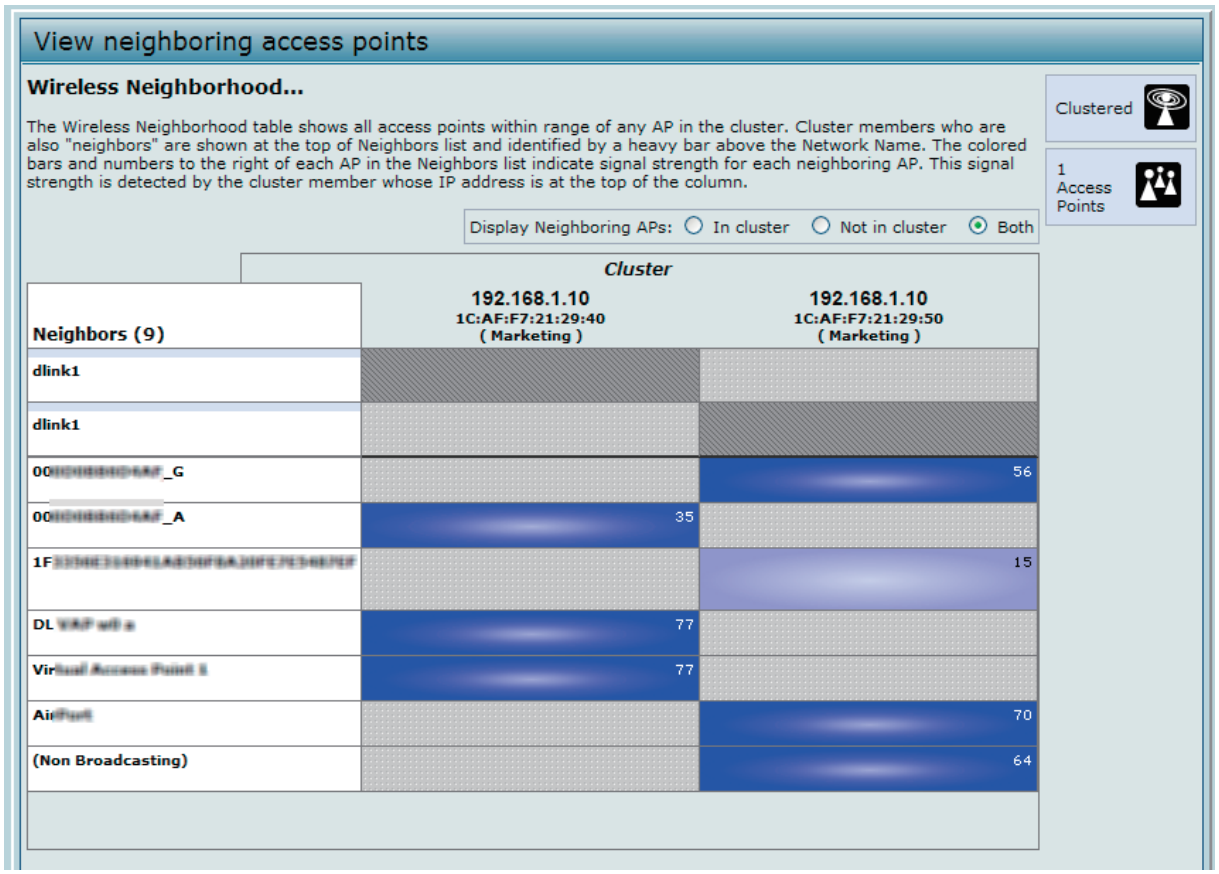


図 10-7　Neighbor アクセスポイントの参照 画面

以下の近接無線デバイス情報が表示されます。

項目	説明
Display Neighboring APs	以下のラジオボタンの 1 つをクリックして、画面を変更します。 • In cluster - クラスタのメンバである Neighbor AP だけを表示します。 • Not in cluster - クラスタメンバではない Neighbor AP だけを表示します。 • Both - すべての Neighbor AP（クラスタメンバとクラスタメンバではないもの）を表示します。
Cluster	テーブルの上部にあるクラスリストではクラスタ内の全アクセスポイントの IP アドレスを表示します。（これは、**Cluster > Access Points** メニューで表示されるクラスタメンバのリストと同じです。） クラスタに 1 つのアクセスポイントしかないと、ここでは 1 つの IP アドレス欄だけが表示され、アクセスポイントが自身にクラスタリングしていることを示します。特定のアクセスポイントに関するその他の詳細を参照するためには、IP アドレスをクリックします。
Neighbors	クラスタリングしている 1 つ以上のアクセスポイントの Neighbor アクセスポイントは、SSID（ネットワーク名）ごとに表示されます。 クラスタメンバの Neighbor として検出されるアクセスポイントは、クラスタメンバ自身である可能性もあります。クラスタメンバである Neighbor は上のリストの先頭に常に表示され、ロケーション表示もあります。 Neighbor リスト内の各アクセスポイントの右側にあるカラーバーは、IP アドレスが欄の先頭に表示されているクラスタメンバにより検出された各 Neighbor AP の信号強度を示しています。 バーのカラーは以下の信号強度を示しています。 • 濃い青色のバー - 濃い青色のバーと高い信号強度番号（例えば、50）は、IP アドレスが欄の上に表示されているアクセスポイントが参照した Neighbor から検出された良好な信号強度を示します。 • 薄い青色のバー - 薄い青色のバーと低い信号強度番号（例えば、20 以下）は、IP アドレスが欄の上に表示されているアクセスポイントが参照した Neighbor から検出された中間または弱い信号強度を示します。 • 白いバー - 白いバーと番号「0」は、クラスタメンバの 1 つが検出した Neighbor AP を IP アドレスがその欄の上に表示されているアクセスポイントでは検出できないことを示します。 • 薄いグレーのバー - 信号強度の表示がグレーのバーは、IP アドレスがその欄の上に表示されているアクセスポイントではなく、他のクラスタメンバによって検出された Neighbor を示します。 • 濃いグレーのバー - 信号強度の表示が濃いグレーのバーは、アクセスポイントが自身を検出する方法を参照するためには適用しないため、IP アドレスがその欄の上に表示されているアクセスポイントであることを示します。

クラスタメンバに関する詳細の参照

クラスタメンバのアクセスポイントに関する詳細情報を参照するためには、画面先頭にあるクラスタメンバの IP アドレスをクリックします。

以下の図は IP アドレス「10.27.65.169」を持つアクセスポイントにおける「Radio 1」の Neighbor の詳細を示しています。

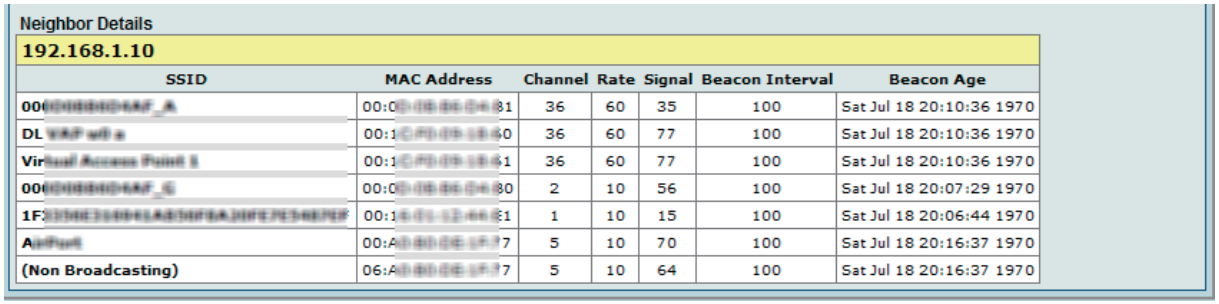


図 10-8　Neighbor アクセスポイントの詳細の参照 画面

以下の表で、選択したアクセスポイントに関する詳細を説明します。

項目	説明
SSID	アクセスポイントの識別子。SSID は、無線ローカルエリアネットワークを特定する 32 文字以内の半角英数字の文字列です。また、ネットワーク名としても参照されます。同じアクセスポイントで動作する Guest ネットワークと内部ネットワークは 2 つの異なるネットワーク名を持つ必要があります。
MAC Address	近接するアクセスポイントの MAC アドレスを表示します。MAC アドレスは、ネットワーク上の各ノードを特定するハードウェアアドレスです。
Channel	アクセスポイントが現在ブロードキャストを行っているチャンネルを示します。チャンネルとは、無線インタフェースがデータの送受信に使用する無線スペクトラムのある一部分を定義するものです。
Rate	アクセスポイントの現在の送信速度（Mbit/s）を示します。現在の送信速度は常に「Supported Rates」に示される速度の 1 つになります。
Signal	このアクセスポイントが出力する信号強度（Db）が表示されます。
Beacon Interval	このアクセスポイントによって使用されるビーコン間隔を示します。ビーコンフレームは無線ネットワークの存在を通知するために、アクセスポイントから定期的に送信されます。初期状態では、ビーコンフレームは 100 ミリ秒に 1 度（1 秒に 10 回）送信されます。
Beacon Age	このアクセスポイントが最後のビーコンを受信した日時を表示します。

第 11 章　ツールメニュー

ツールメニューには以下のものがあります。

項目	説明
Home	本製品の現在の基本情報を表示します。**Basic Setting** をクリックしてアクセスすることもできます。詳しくは「Basic Settings（デバイス情報）」（30 ページ）を参照してください。
Tools	以下のメニューがあります。 • Basic Settings - 本製品の現在の基本情報を表示します。**Basic Setting** をクリックしてアクセスすることもできます。詳しくは「Basic Settings（デバイス情報）」（30 ページ）を参照してください。 • Upgrade - 本製品のファームウェアを更新します。**Maintenance > Upgrade** の順にクリックしてアクセスすることもできます。詳しくは「Upgrade（ファームウェアの更新）」（104 ページ）を参照してください。 • SNTP - NTP を使用してクロックタイムを同期させます。**Services > Time** の順にクリックしてアクセスすることもできます。詳しくは「Time（NTP サーバの有効化）」（94 ページ）を参照してください。
Configuration	以下のメニューがあります。 • Configuration Save - 現在のコンフィグレーションファイルを保存します。**Maintenance > Configuration Save** の順にクリックしてアクセスすることもできます。詳しくは「Configuration Save（コンフィグレーションの保存）」（99 ページ）を参照してください。 • Configuration Restore - 保存したコンフィグレーションをリストアします。**Maintenance > Configuration Restore** の順にクリックしてアクセスすることもできます。詳しくは「Configuration Restore（コンフィグレーションのリストア）」（101 ページ）を参照してください。
System	本製品の工場出荷時設定へのリセット、および再起動を行います。**Maintenance > Maintenance** の順にクリックしてアクセスすることもできます。詳しくは「Maintenance（リセットと再起動）」（103 ページ）を参照してください。
Help	各機能に関するヘルプ情報を表示します。

付録 A　設定例

この付録では D-Link 統合アクセスシステムのソフトウェアで利用可能ないくつかの機能を設定する方法例を説明します。各例には、Web インタフェース、CLI、および SNMP を使用することで機能を設定する方法に関する手順があります。この付録では以下の手順を行う方法を説明しています。

- VAP の設定
- 無線設定
- WDS の設定
- アクセスポイントのクラスタリング
- クライアント QoS の設定

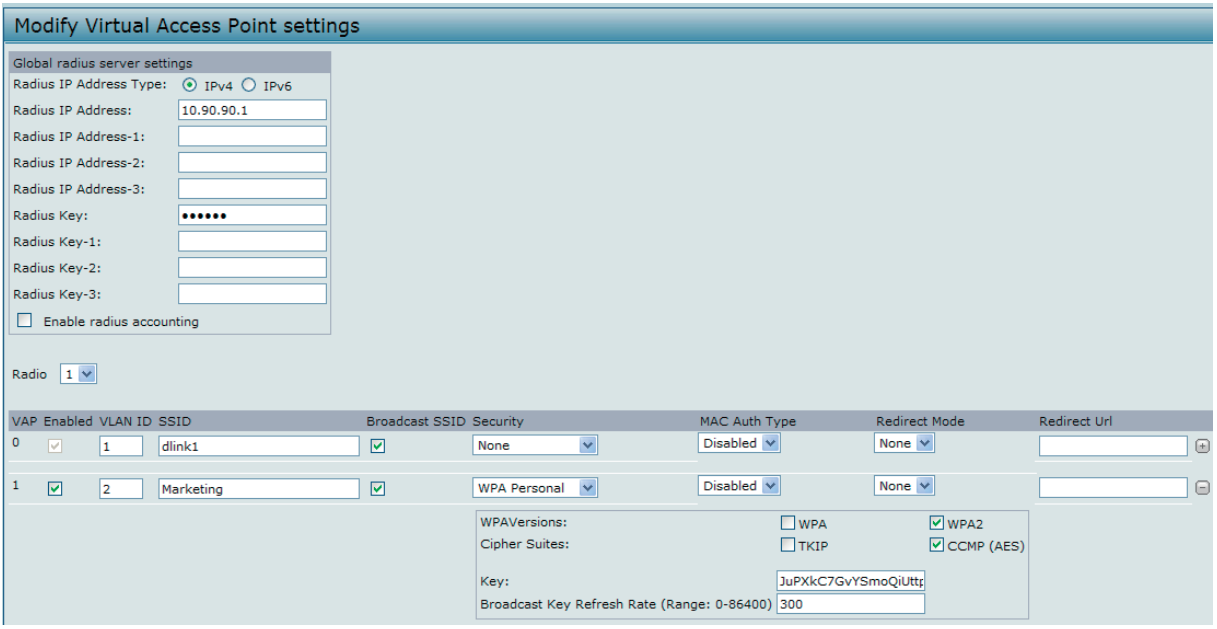
VAP の設定

この例題では、以下のように VAP 1 の設定を初期設定から変更します。

- VLAN ID : 2
- SSID : Marketing
- Security : WPA Personal using WPA2 with CCMP (AES)

Web インタフェースからの VAP 設定

1. 本製品にログインし、ナビゲーションツリーから **Manage > VAP** の順にメニューをクリックします。


Modify Virtual Access Point settings
Global radius server settings
Radius IP Address Type: IPv4 IPv6
Radius IP Address: 10.90.90.1
Radius IP Address-1:
Radius IP Address-2:
Radius IP Address-3:
Radius Key:
Radius Key-1:
Radius Key-2:
Radius Key-3:
Enable radius accounting
Radio 1
VAP Enabled VLAN ID SSID Broadcast SSID Security MAC Auth Type Redirect Mode Redirect Url
0 1 dlink1 None Disabled None
1 2 Marketing WPA Personal Disabled None
WPAVersions: WPA WPA2
Cipher Suites: TKIP CCMP (AES)
Key: JuPXkC7GvYSmoQiUtt
Broadcast Key Refresh Rate (Range: 0-86400) 300

2. VAP 1 の「Enabled」欄のチェックボックスをチェックします。

3. 「VLAN ID」欄に「2」を入力します。

4. 「SSID」欄で既存の SSID を削除して「Marketing」と入力します。

5. 「Security」欄のプルダウンメニューから「WPA Personal」を選択します。
新しい項目が表示されます。

6. 「WPA2」と「CCMP（AES）」のチェックボックスをチェックし、「WPA」と「TKIP」のチェックを外します。

7. 「Key」欄に WPA 暗号キーを入力します。
暗号キーには、半角英数字および記号を使用することができます。暗号キーは、大文字小文字を区別し、8 ～ 63 文字です。

8. 「Apply」ボタンをクリックし、新しい設定を適用します。

CLI からの VAP 設定

1. Telnet、SSH、またはシリアル接続を使用して本製品を CLI に接続します。

2. VAP 1 を有効にします。

```
set vap vap1 status up
```

3. VLAN ID を「2」に設定します。

```
set vap vap1 vlan-id 2
```

注意 上記のコマンドでは、両方の無線デバイスの「VAP 1」の「VLAN ID」を「2」に設定します。Radio 1 における「VAP 1」の「VLAN ID」だけを設定する場合は、次のコマンドを使用します。

```
set vap 1 with radio wlan0 to vlan-id 2
```

4. SSID を「Marketing」に設定します。

```
set interface wlan0vap1 ssid Marketing
```

5. セキュリティモードを「WPA Personal」に設定します。

```
set interface wlan0vap1 security wpa-personal
```

6. 本製品への接続を WPA2 クライアントに許可し、WPA クライアントを拒否します。

```
set bss wlan0bssvap1 wpa-allowed off
set bss wlan0bssvap1 wpa2-allowed on
```

7. Cipher Suite（暗号スイート）を「CCMP（AES）」のみに設定します。

```
set bss wlan0bssvap1 wpa-cipher-tkip off
set bss wlan0bssvap1 wpa-cipher-ccmp on
```

8. 事前共有鍵を設定します。

```
set interface wlan0vap1 wpa-personal-key JuPXkC7GvY$moQiUttp2
```

事前共有鍵にスペースが含まれている場合は、キーの前後に「"」を入力します。

9. 次のコマンドを使用して設定の参照と確認を行います。

```
DLINK-WLAN-AP# get interface wlan0vap1 detail
Property                Value
------------------------------------------------------
type                    service-set
status                  up
description             Wireless - Virtual Access Point 1
mac                     1C:AF:F7:21:29:41
ip
mask
static-ip
static-mask
rx-bytes                0
rx-packets              0
rx-errors               0
tx-bytes                11188
tx-packets              64
tx-errors               0
tx-drop-bytes           0
rx-drop-bytes           0
tx-drop-packets         0
rx-drop-packets         0
priority
port-isolation
ssid                    Marketing
```

```
bss                     wlan0bssvap1
security                wpa-personal
wpa-personal-key        JuPXkC7GvYSmoQiUttp2
wep-key-ascii           no
wep-key-length          104
wep-default-key         1
wep-key-1
wep-key-2
wep-key-3
wep-key-4
wep-key-mapping-length  400
vlan-interface
vlan-id
radio
remote-mac
wep-key
operational-status
wds-ssid
wds-security-policy
wds-wpa-psk-key
```

```
DLINK-WLAN-AP# get vap vap1 detail
Property          Value
-------------------------------------------------
radio             wlan0
status            up
vlan-id           2
global-radius     on
description       Virtual Access Point 1
redirect-mode     none
redirect-url
qos-mode          down
def-bwmax-up      0
def-bwmax-down    0
def-acltype-up    none
def-acltype-down  none
def-acl-up
def-acl-down
def-policy-up
def-policy-down

Property          Value
-------------------------------------------------
radio             wlan1
status            up
vlan-id           2
global-radius     on
description       Virtual Access Point 1 - Radio 2
redirect-mode     none
redirect-url
qos-mode          down
def-bwmax-up      0
def-bwmax-down    0
def-acltype-up    none
def-acltype-down  none
def-acl-up
def-acl-down
def-policy-up
def-policy-down
DLINK-WLAN-AP#
```

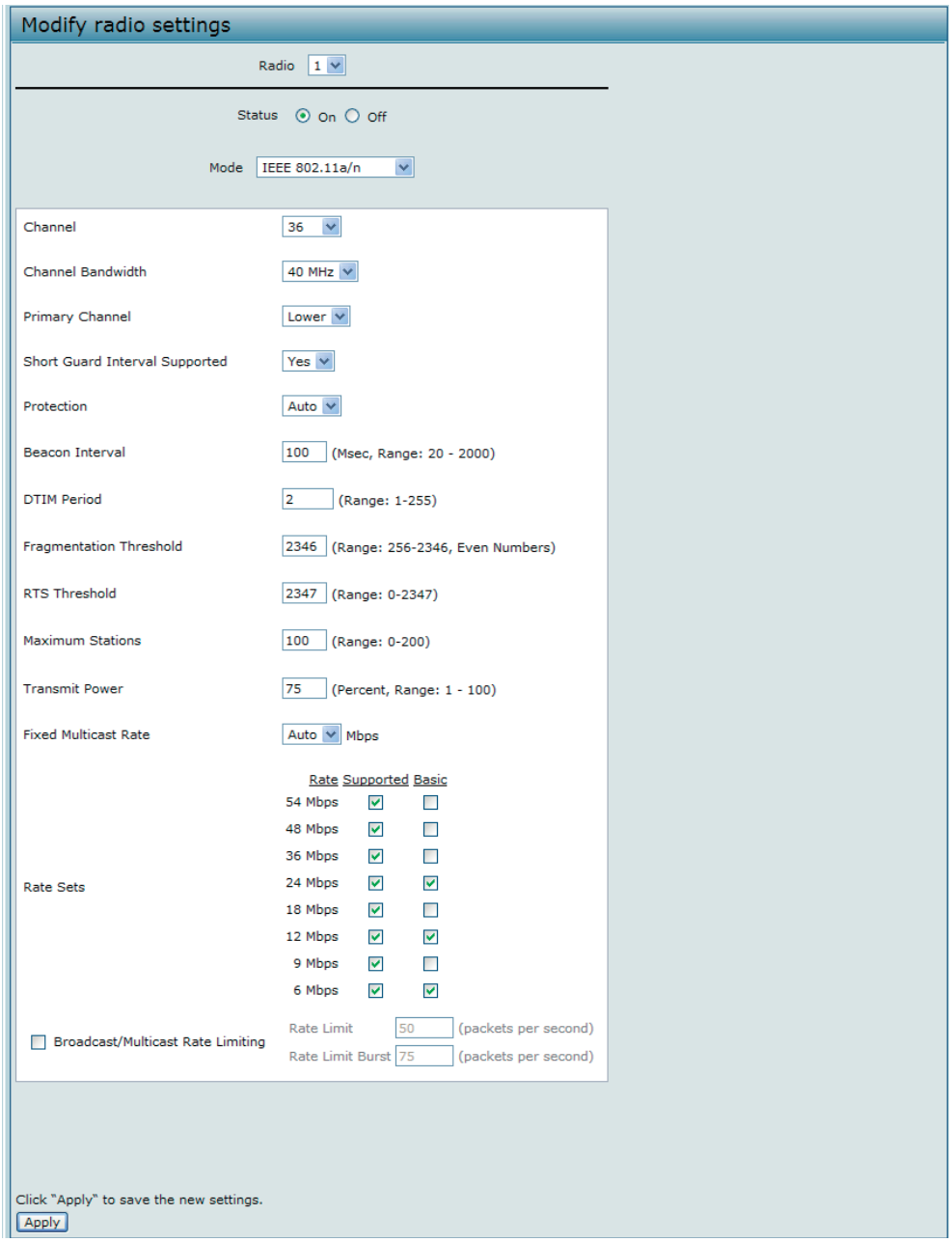
無線インタフェースの設定

本例題では、以下の設定を使用して Radio 1 を設定する方法を示します。

- モード - IEEE 802.11a/n
- チャンネル - 36
- チャンネル帯域幅 - 40MHz
- 最小ステーション - 100
- 送信電力 - 75%

Web インタフェースからの無線インタフェース設定

1. アクセスポイントにログインし、**Manage > Radio** 画面を表示します。
2. 番号「1」が「Radio」欄に表示され、ステータスが「On」であることを確認します。
3. 「Mode」メニューから「IEEE 802.11a/n」を選択します。
4. 「Channel」欄から「36」を選択します。
5. 「Channel Bandwidth」欄から「40MHz」を選択します。
6. 「Maximum Station」欄の値を「100」に変更します。
7. 「Transmit Power」欄の値を「75」に変更します。



8. 「Update」ボタンをクリックし、新しい設定を適用します。

CLI を使用した無線設定

1. Telnet、SSH、またはシリアル接続を使用してアクセスポイントに接続します。

2. ステータスが現在 up でない場合、Radio 1 を有効にします。

```
set radio wlan0 status Up
```

3. モードを IEEE 802.11a/n に設定します。

```
set radio wlan0 mode a-n
```

4. チャンネルを 36 に設定します。

```
set radio wlan0 channel-policy static
set radio wlan0 static-channel 36
```

5. チャンネル帯域幅を 40MHz に設定します。

```
set radio wlan0 n-bandwidth 40
```

6. 一度に最大 100 個のステーションをアクセスポイントに接続させます。

```
set bss wlan0bssvap0 max-stations 100
```

7. 送信電力を 75% に設定します。

```
set radio wlan0 tx-power 75
```

8. 無線設定に関する情報を参照します。

```
DLINK-WLAN-AP# get radio wlan0 detail
Property                        Value
------------------------------------------
status                          up
description                     IEEE 802.11a
channel-policy                  static
mode                            a-n
static-channel                  36
channel                         36
tx-power                        75
beacon-interval                 100
rts-threshold                   2347
fragmentation-threshold         2346
n-bandwidth                     40
n-primary-channel               lower
protection                      auto
short-guard-interval-supported  yes
station-isolation               off
rate-limit-enable               off
rate-limit                      50
rate-limit-burst                75
wlan-util                       1
fixed-multicast-rate            auto
DLINK-WLAN-AP#
```

WDS の設定

本例では、2 つのアクセスポイント間に WDS リンクを設定する方法を示しています。ローカルなアクセスは MAC アドレス「00:1B:E9:16:32:40」を持つ「MyAP1」で、リモートアクセスポイントは MAC アドレス「00:30:AB:00:00:B0」を持つ「MyAP2」とします。

WDS リンクには、以下の設定があり、両方のアクセスポイントに設定される必要があります。

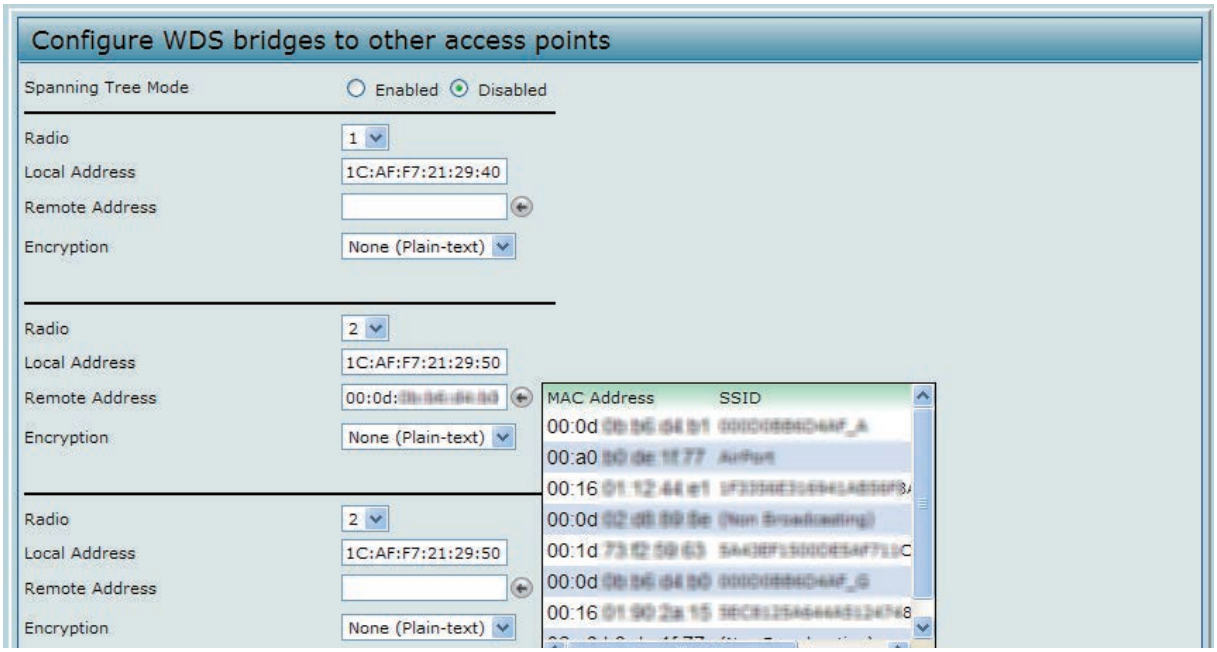
- 暗号化 - WPA(PSK)
- SSID - wds-link
- Key - abcdefghijk

Web インタフェースからの WDS 設定

1 組のアクセスポイント間に WDS リンク「MyAP1」および「MyAP2」を作成するためには、以下の手順を使用します。

1. 「MyAP1」にログインし、**Manage > WDS** 画面を表示します。
「MyAP1」の MAC アドレスが自動的に MyAP1（現在参照しているアクセスポイント）「Local Address」欄に表示されます。

2. 「Remote Address」欄に「MyAp2」の MAC アドレスを入力するか、欄の横にある矢印をクリックして表示されるメニューから「MyAp2」の MAC アドレスを選択します。

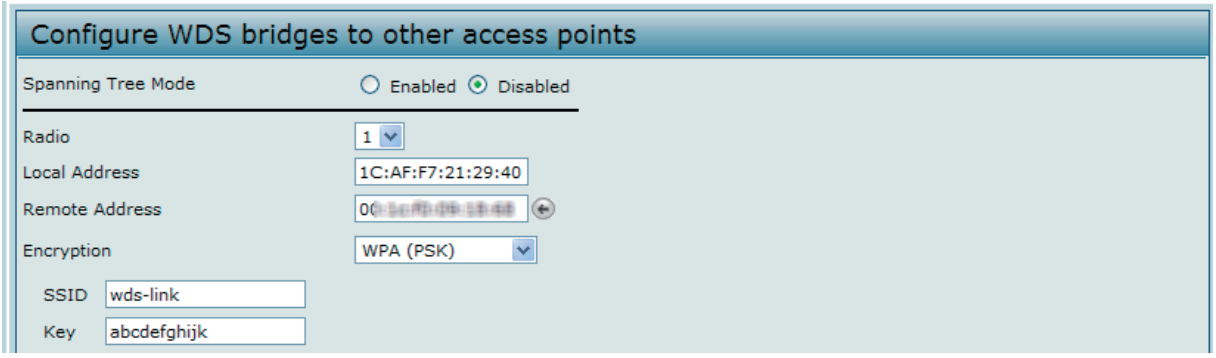


3. 「Encryption」メニューから「WPA(PSK)」を選択します。

注意 「Radio 1」における VAP0 が WPA (PSK) を使用する場合にだけ、WPA(PSK) オプションはセキュリティ方式として利用可能です。VAP0 が WPA Personal または WPA Enterprise に設定されない場合、None (Plain-text) または WDS link encryption のどちらかを選択する必要があります。

4. 「SSID」に「wds-link」、「Key」に「abcdefghijk」と入力します。

5. 「Update」ボタンをクリックしてアクセスポイントに WDS 設定を適用します。



6. 「MyAP2」にログインし、手順 2-5 を繰り返します。ただし、「Remote Address」欄には「MyAP1」の MAC アドレスを使用することに注意します。

注意 MyAP1 と MyAP2 は同じ IEEE 802.11 モードで、同じチャンネルで送信するように設定される必要があります。

CLI を使用した WDS 設定

1. Telnet、SSH、またはシリアル接続を使用して「MyAP1」に接続します。

2. 「MyAP2」のリモート MAC アドレスを設定します。

```
set interface wlan0wds0 status up remote-mac 00:30:AB:00:00:B0
```

3. リンクの暗号化タイプとして「WPA(PSK)」を設定します。

```
set interface wlan0wds0 wds-security-policy wpa-personal
```

4. WDS リンクにおける SSID を設定します。

```
set interface wlan0wds0 wds-ssid wds-link
```

5. 暗号化キーを設定します。

```
set interface wlan0wds0 wds-wpa-psk-key abcdefghijk
```

6. WDS リンクを管理上有効にします。

```
set interface wlan0wds0 status up
```

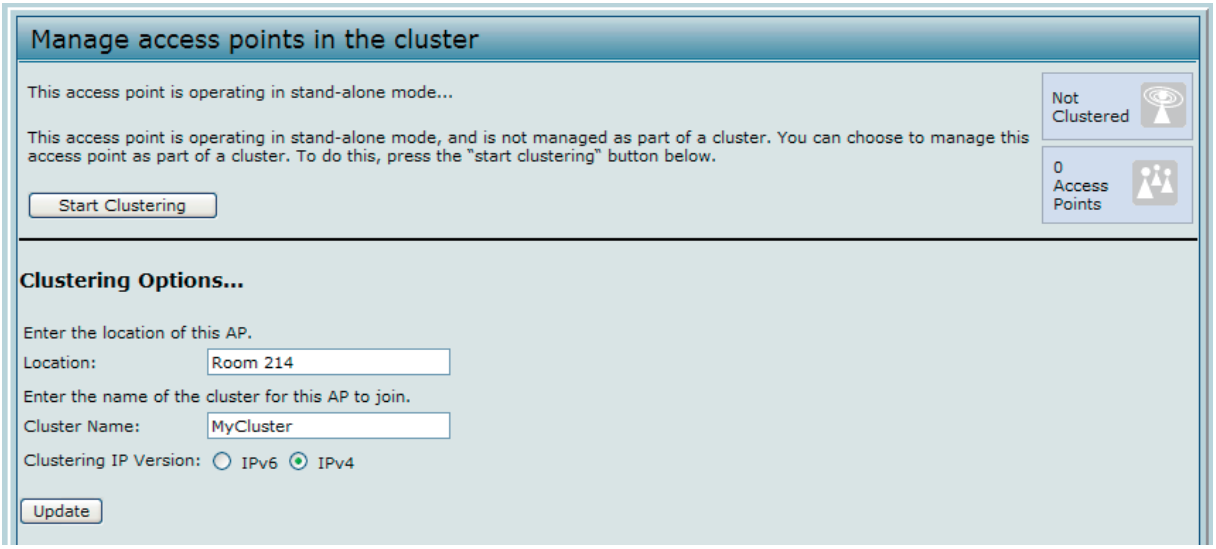
7. 同じ設定手順を MyAP2 にも実行します。

アクセスポイントのクラスタリング

本例では、2 つのアクセスポイント間にクラスタを設定し、自動チャンネル再割り当てを有効にする方法を示しています。ローカルなアクセスポイントのロケーションは「Room214」で、クラスタ名は「MyCluster」であるものとします。

Web インタフェースを使用したアクセスポイントのクラスタリング

1. アクセスポイントにログインし、**Cluster > Access Points** 画面を表示します。

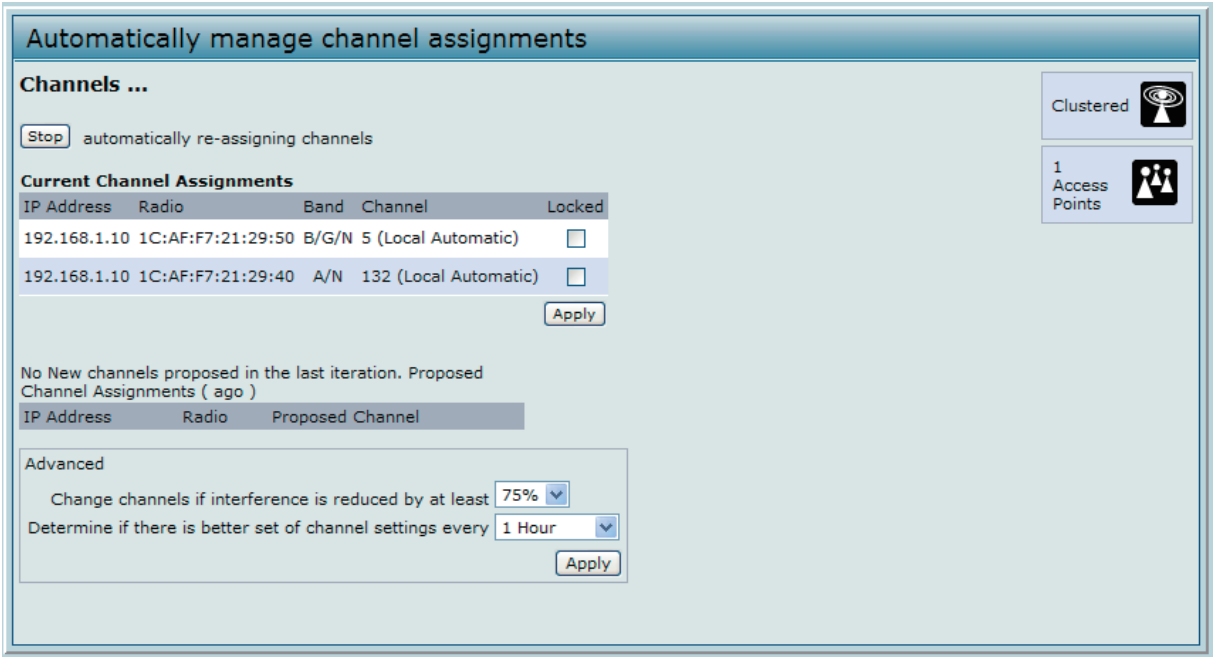


2. アクセスポイントが接続するロケーションと参加するクラスタの名称を入力します。

3. 「Update」ボタンをクリックします。

4. 「Start Clustering」ボタンをクリックして、クラスタリング機能を有効にします。
画面の更新後、同じブリッジセグメントにあり、同じ操作モードの無線帯域を持ち、クラスタリングが有効で、同じクラスタ名を持つ他のアクセスポイントがアクセスポイントテーブルに表示されます。

5. 「Channel Management」画面を表示してチャンネル割り当てを参照します。
現在のチャンネル割り当てと提案されたチャンネル割り当てを表示します。「Advanced」セクションの間隔設定では、提案された変更を適用する間隔を決定します。



CLI を使用したクラスタリングアクセスポイントの設定

1. Telnet、SSH、またはシリアル接続を使用してアクセスポイントに接続します。

2. アクセスポイントのロケーションを設定します。

```
set cluster location "Room 214"
```

注意 クラスタ名かクラスタロケーションがスペースを持つ場合、コマンド例の通り、CLI でテキストを入力する際に「"」マークでテキストを囲む必要があります。Web UI を使用してテキストを入力する場合には、「"」マークを使用する必要はありません。

3. クラスタ名を設定します。

```
set cluster cluster-name MyCluster
```

4. クラスタリングを開始します。

```
set cluster clustered 1
```

5. アクセスポイントのクラスタリング設定に関する情報を参照します。

```
DLINK-WLAN-AP# get cluster detail
Property      Value
----------------------
clustered     1
location      Room 214
cluster-name  MyCluster
ipversion     ipv4
DLINK-WLAN-AP#
```

6. 自動チャンネルプランを開始します。

```
set channel-planner status up
```

7. 自動チャンネルプランの設定を参照します。

```
DLINK-WLAN-AP# get channel-planner detail
Property          Value
----------------------
status            up
change-threshold  75
interval          60
locked-ips
DLINK-WLAN-AP#
```

クライアント QoS の設定

この例ではクライアント QoS を有効にする方法、アクセスポイントに ACL と DiffServ ポリシーを設定する方法、VAP2 に接続するクライアントから送信されるトラフィックおよびアクセスポイントが受信するトラフィックに ACL とポリシーを適用する方法について示します。

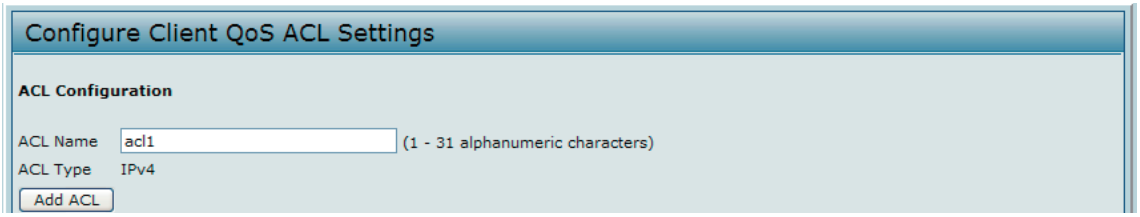
IPv4 ACL は「acl1」という名称で、2 つのルールを含むものとします。最初のルールは、「192.168.1.0」サブネットからの HTTP トラフィックを許可します。2 番目のルールは管理ステーション「192.168.1.23」からの全 IP トラフィックを許可します。他のすべてのトラフィックは、ACL リストの最後にある暗黙の「deny all」（すべて拒否）のルールで拒否されます。ACL は、アクセスポイントが接続するクライアントからトラフィックを受信する場合にパケットがチェックされるように、アクセスポイントの内向きインタフェースに適用されます。

この例の DiffServ ポリシーは、RADIUS サーバを通じて DiffServ ポリシー名を取得しない VAP に接続するクライアントに対して初期値で行う DiffServ の動作を示します。宛先アドレス（192.168.2.200）として VoIP サーバを持つ「192.168.1.0」サブネットがクライアントから受信した音声トラフィック（UDP パケット）は、他のトラフィックより優先するように「EF」（完全優先転送）の IP DSCP 値でマークされます。

Web インタフェースを使用した QoS 設定

ACL の設定

1. アクセスポイントにログインし、**Client QoS > Client QoS ACL** 画面を表示します。



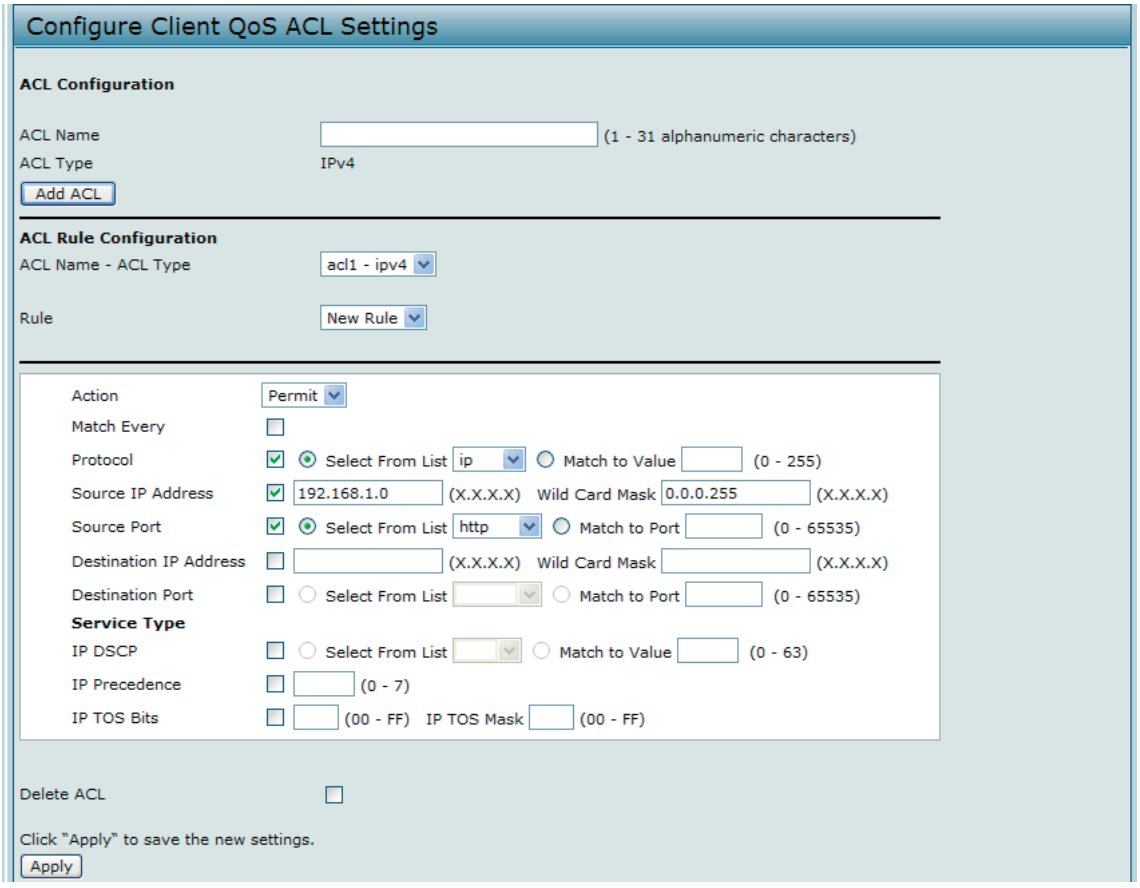
2. 「ACL Name」欄に「acl1」を入力し、「Add ACL」ボタンをクリックします。

3. 「Action」メニューから「Permit」を選択します。

4. 「Match Every」オプションをクリアします。

5. 「Protocol」オプションが選択され、「Select From List」メニューから「ip」が選択されることを確認します。

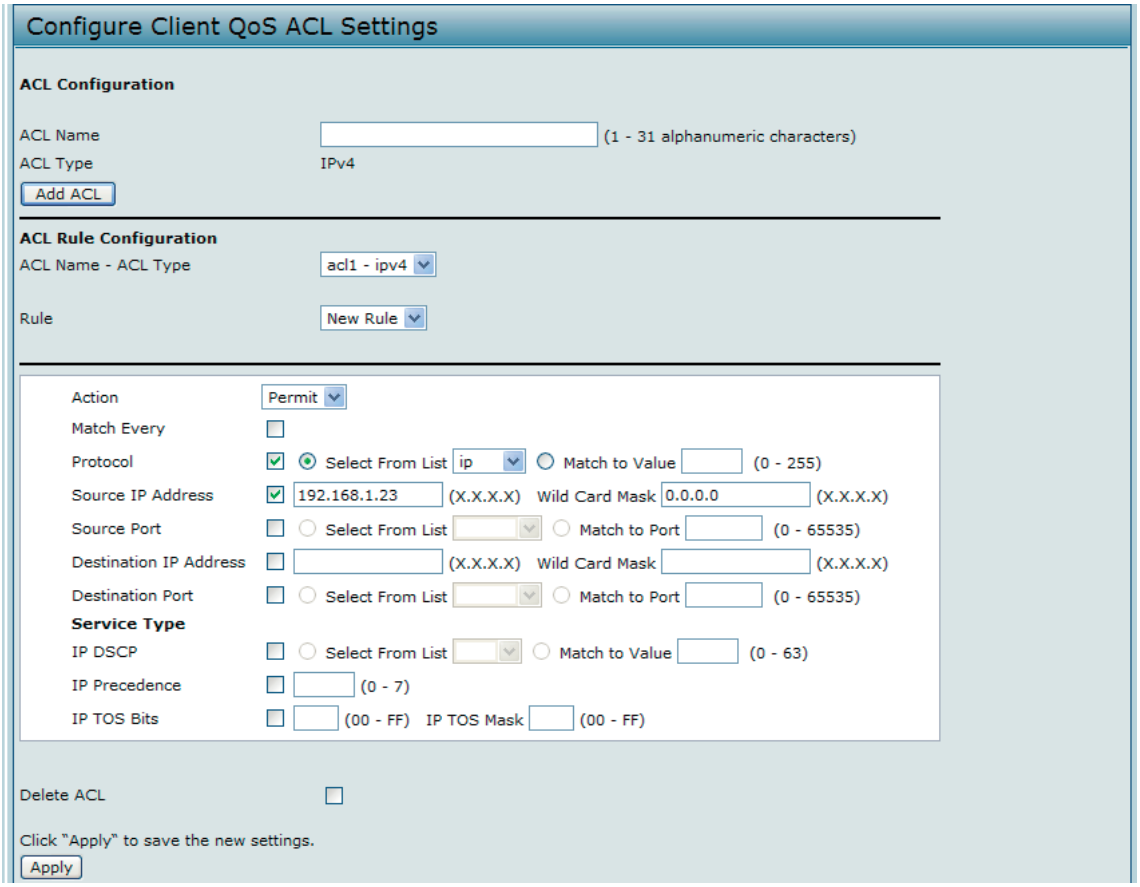
6. 残りの設定を行います。



- Source IP Address : 192.168.1.0
- Wild Card Mask : 0.0.0.255
- Source Port : オプションを選択します。
- Select From List (Source Port) : http

7. 「Apply」ボタンをクリックして、ルールを保存します。

8. 「Rule」メニューから「New Rule」を選択し、以下の設定を持つ別のルールを作成します。



- Action : Permit
- Match Every : オプションをクリアします。
- Protocol - Select From List : ip
- Address : 192.168.1.23
- Wild Card Mask : 0.0.0.0

9. 「Apply」ボタンをクリックして、ルールを保存します。

10. アクセスポイントにログインし、**Client QoS > VAP QoS Parameters** 画面を表示します。

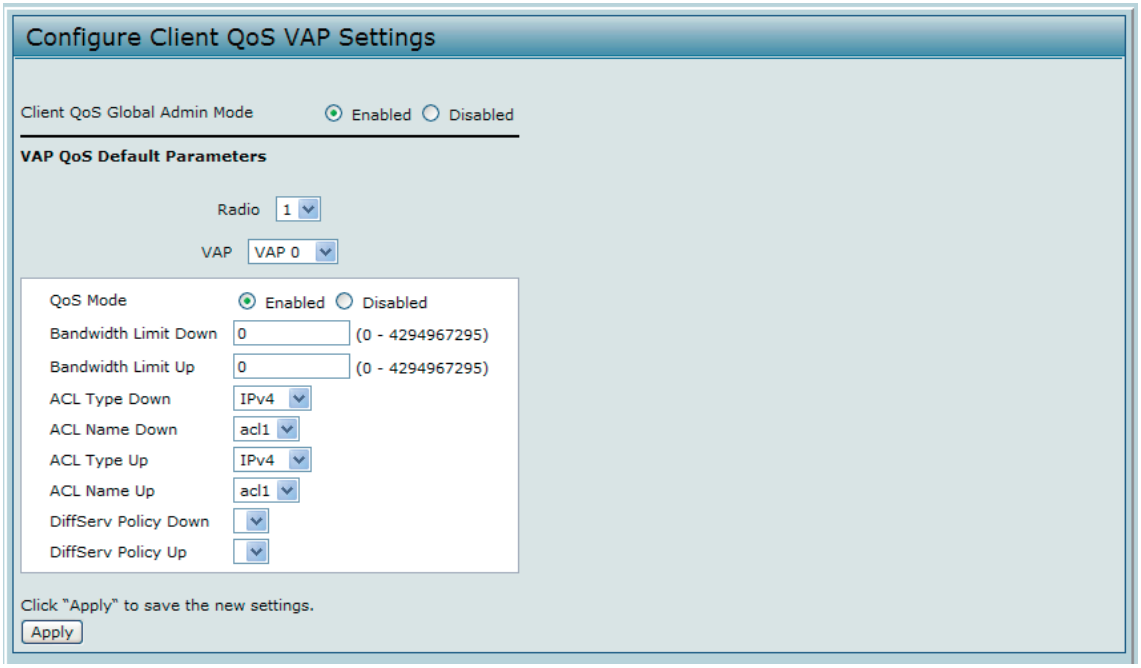
11. 「Client QoS Global Admin Mode」オプションから、「Enabled」を選択します。

12. 「VAP」メニューから「VAP 0」を選択します。

13. 「QoS Mode」に「Enabled」オプションを選択します。

14. 「ACL Type Up」メニューから、「IPv4」を選択します。

15. 「ACL Name Up」メニューから、「acl1」を選択します。

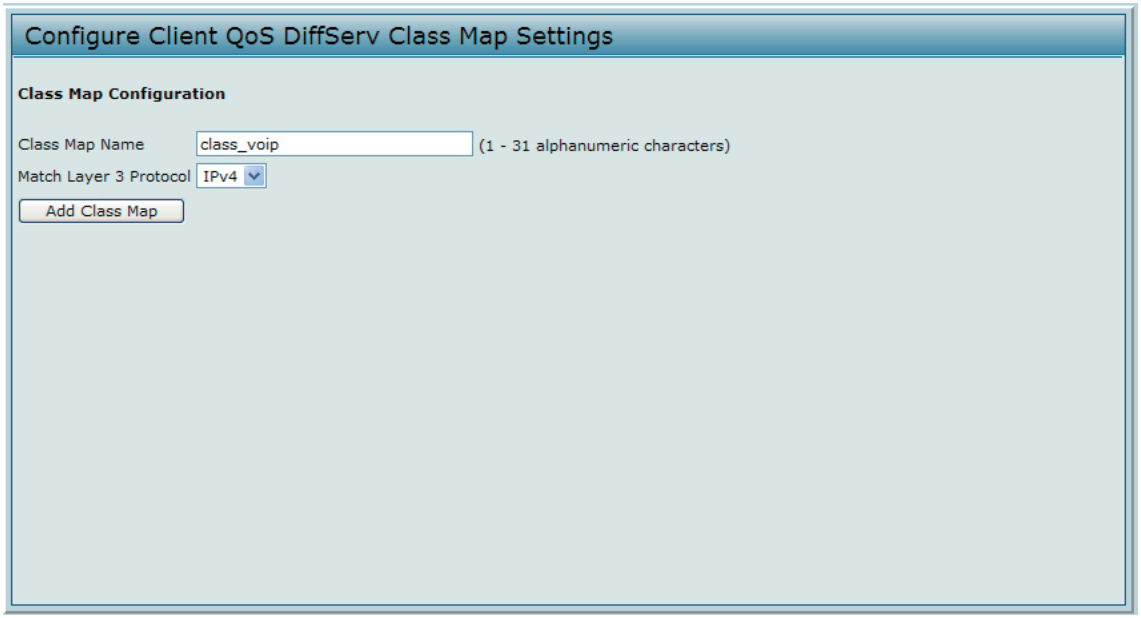


16. 「Apply」ボタンをクリックし、QoS 設定をアクセスポイントに適用します。

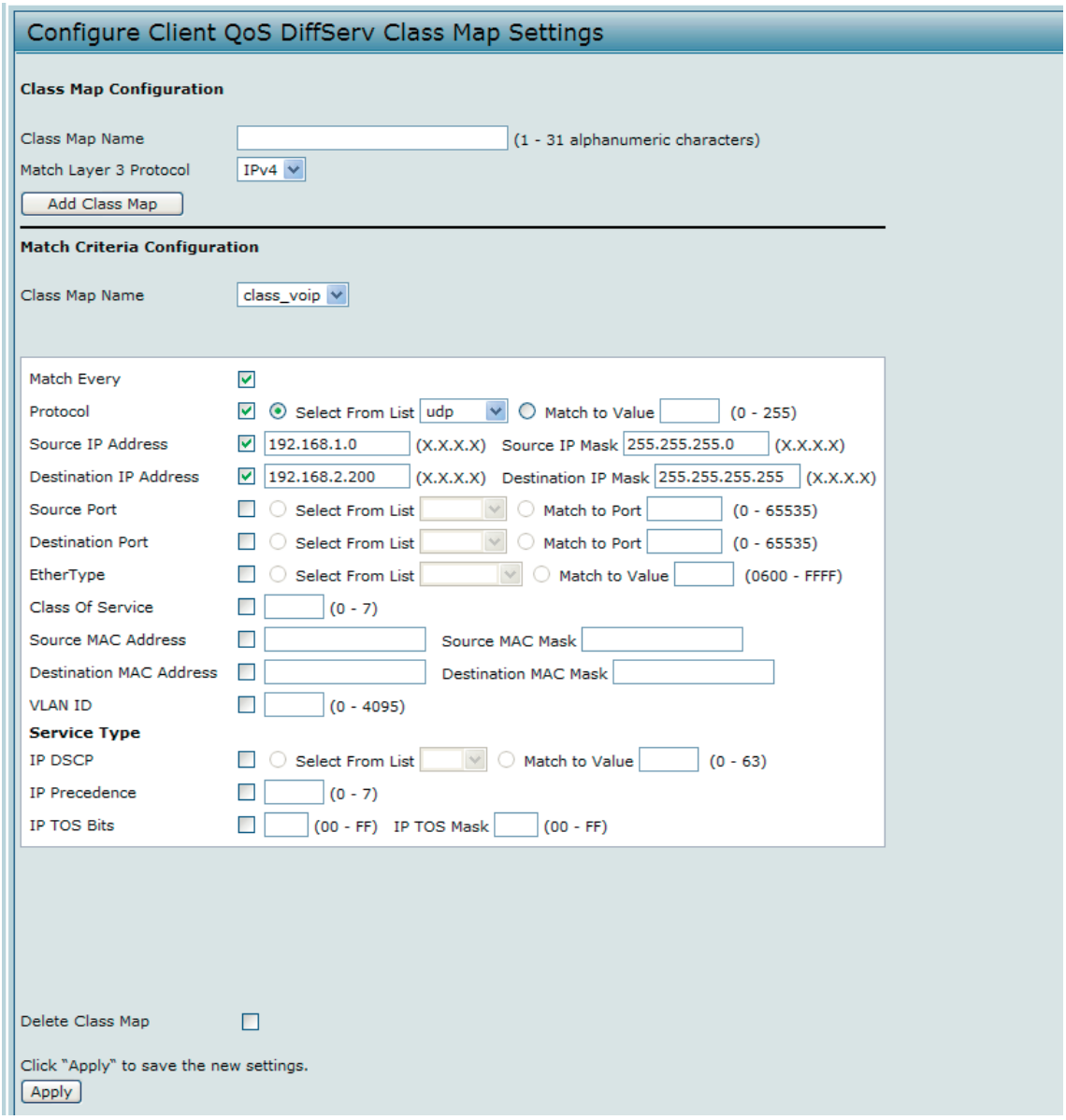
Diffserv 設定

1. アクセスポイントにログインし、**Client QoS > Class Map** 画面を表示します。

2. 「Class Map Name」欄に「class_voip」を入力し、「Add Class Map」ボタンをクリックします。



画面は更新され、追加の項目が表示されます。



3. パケットが一致していると見なすために、「Match Every」オプションを選択して、クラスに定義されたすべての一致基準を満たす必要があることを示します。

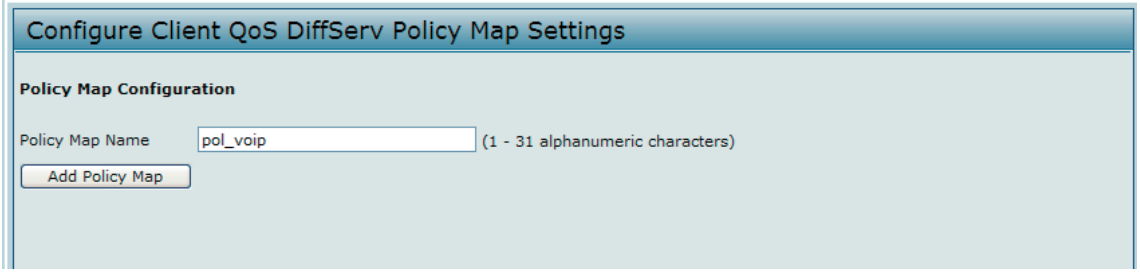
4. 「Protocol」選択し、次に「Select From List」から「udp」を選択して照合する基準と UDP を定義します。

5. 「Source IP Address」を選択し、以下の情報を入力します。
- Address : 192.168.1.0
- Source IP Mask : 255.255.255.0

6. 「Destination IP Address」オプションを選択し、VoIP サーバに以下の情報を入力します。
- Address : 192.168.2.200
- Destination IP Mask : 255.255.255.255

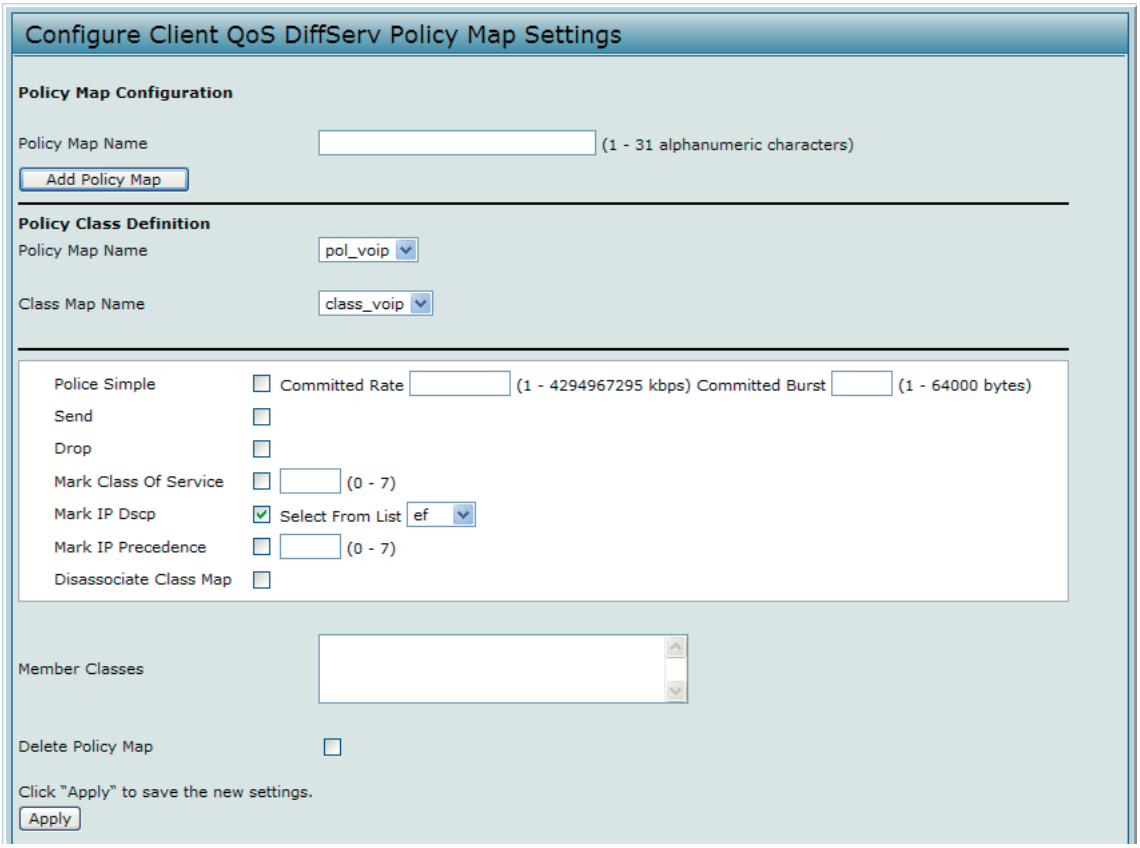
7. 「Apply」ボタンをクリックして、照合基準を保存します。

8. **Client QoS > Policy Map** 画面を表示します。



9. ポリシー作成するためには、「Policy Map Name」欄に「pol_voip」を入力し、「Add Policy Map」ボタンをクリックします。
画面は更新され、追加の項目が表示されます。

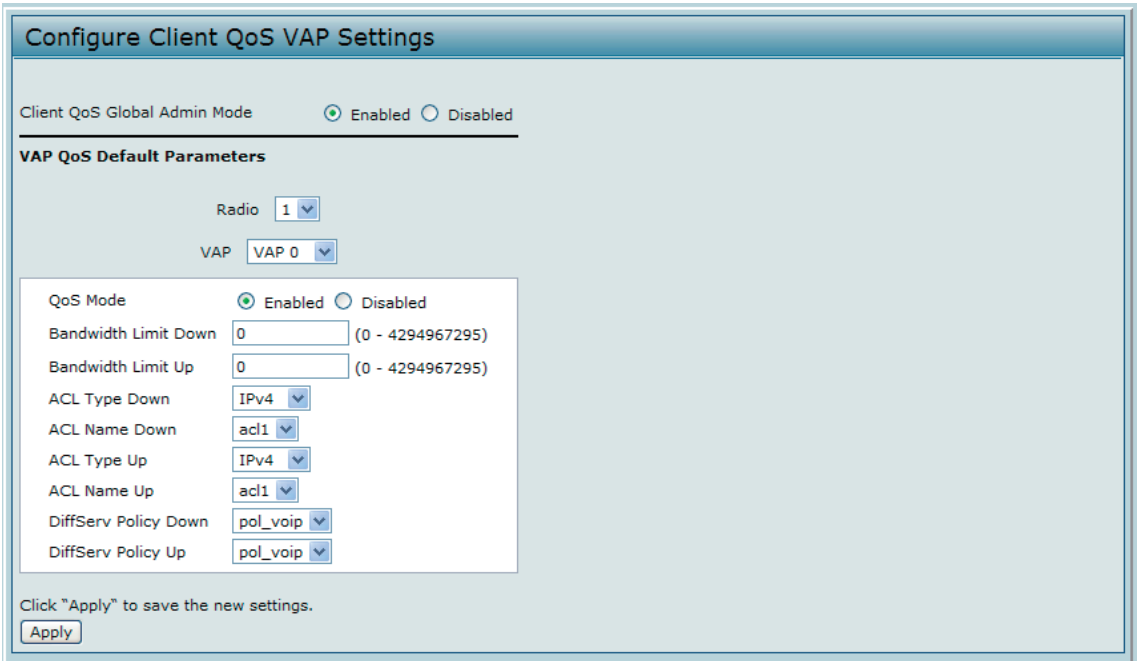
10. クラスマップ「class_voip」のために、「Mark IP Dscp」オプションを選択し、次に「Select From List」メニューから「ef」を選択します。
「class_voip」クラスに定義された基準を満たすトラフィックは、EF（完全優先転送）の DSCP 値でマークされます。



11.「Apply」ボタンをクリックして、設定を適用します。

12. **Client QoS > VAP QoS Parameters** 画面を表示します。

13. 「VAP」メニューから「VAP0」を選択します。



14. 「Client QoS Global Admin Mode」と「QoS Mode」が共に有効であることを確認し、以下の情報を入力します。

- ACL Type Down : IPv4
- ACL Name Down : acl1
- ACL Type Up : IPv4
- ACL Name Up : IPv4
- DiffServ Policy Down : pol_voip
- DiffServ Policy Up : pol_voip

15. 「Apply」ボタンをクリックし、QoS 設定をアクセスポイントに適用します。

CLI を使用した QoS 設定

ACL 設定

1. アクセスポイントに接続します。

2. 「acl1」という名称の ACL を作成します。

```
add acl acl1 acl-type ipv4
```

3. 「acl1」に 192.168.1.0 サブネットからの HTTP トラフィックを許可するルールを追加します。

```
add rule acl-name acl1 acl-type ipv4 action permit protocol ip src-ip 192.168.1.0
src-ip-mask 0.0.0.255 src-port http
```

4. 「acl1」に IP アドレス 192.168.1.23 を持つホストからの全トラフィックを許可する別のルールを追加します。

```
add rule acl-name acl1 acl-type ipv4 action permit protocol ip src-ip
192.168.1.23 src-ip-mask 0.0.0.0
```

5. アクセスポイントのクライアント QoS を有効にします。

```
set client-qos mode up
```

6. VAP0 に ACL のタイプを指定します。

```
set vap vap0 def-acltype-down ipv4
set vap vap0 def-acltype-up ipv4
```

7. 「acl1」を VAP0 のアクセスコントロールリストに適用します。

```
set vap vap0 def-acl-up acl1
set vap vap0 def-acl-down acl1
```

8. VAP0 でクライアント QoS を有効にします。

```
set vap vap0 qos-mode up
```

Diffserv 設定

1. アクセスポイントに CLI でログインします。

2. 「class_voip」という名称のクラスマップを作成し、「192.168.2.200」（VoIP サーバ）の宛先 IP アドレスを持つ「192.168.1.0」ネットワークからのすべての UDP パケットに一致するように設定します。

```
add class-map class_voip l3-protocol ipv4 every yes protocol udp src-
ip 192.168.1.0 src-ip-mask 255.255.255.0 dst-ip 192.168.2.200 dst-ip-mask
255.255.255.255
```

3. 「pol_voip」という名称のポリシーマップを追加します。

```
add policy-map pol_voip
```

4. 「class_voip」クラスマップを追加し、「class_voip」基準に一致するパケットを EF（完全優先転送）の DSCP 値でマークすることを指定することで「pol_voip」ポリシーマップを定義します。

```
add policy-attr policy-map-name pol_voip class-map-name class_voip mark-ip-dscp ef
police-simple no
```

5. pol_voip を VAP0 に適用します。

```
set vap vap0 def-policy-up pol_voip
set vap vap0 def-policy-down pol_voip
```

6. アクセスポイントのクライアント QoS を有効にします。

```
set vap vap0 qos-mode up
```

付録 B　システムの初期設定

本章では、本製品にあらかじめ設定されている初期値を示します。

B.1 アクセスポイントの初期設定

本製品の初期設定は以下の通りです。

設定項目		初期値
システム情報	ユーザ名	admin
	パスワード	admin
ネットワーク情報	DHCP クライアント	有効
	管理用 IP アドレス	10.90.90.91（DHCP による割り当てがない場合）
	サブネットマスク	255.0.0.0（DHCP による割り当てがない場合）
	DNS 名	なし
	管理用 VLAN ID	1
	タグなし VLAN ID	1
	IPv6 Admin モード	有効
	IPv6 Auto Config Admin モード	有効
無線設定	無線インタフェース（1 と 2）	On
	無線 1 IEEE 802.11 モード	802.11a/n
	無線 2 IEEE 802.11 モード	802.11b/g/n
	802.11b/g/n チャンネル	自動
	無線 1 チャンネル帯域	40 MHz
	無線 2 チャンネル帯域	20 MHz
	802.11a/n チャンネル	自動
	プライマリチャンネル	Lower
	Protection	Auto
	無線クライアント数	200
	Transmit Power	100 %
	ブロードキャスト / マルチキャストレート制限	無効
	Fixed Multicast Rate	自動
	Beacon Interval	100 ミリ秒
	DTIM Period	2 ビーコン
	Fragmentation Threshold	2346 バイト
	RTS Threshold	2347 バイト
	Rate Sets Supported(Mbps)	IEEE 802.11a : 54, 48, 36, 24, 18, 12, 9, 6 IEEE 802.11b : 11, 5.5, 2, 1 IEEE 802.11g : 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 IEEE 5 GHz 802.11n : 54, 48, 36, 24, 18, 12, 9, 6 IEEE 2.4 GHz 802.11g : 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1
	Rate Sets(Mbps) (Basic/Advertised)	IEEE 802.11a : 24, 12, 6 IEEE 802.11b : 2, 1 IEEE 802.11g : 11, 5.5, 2, 1 IEEE 5 GHz 802.11n : 24, 12, 6 IEEE 2.4 GHz 802.11n : 11, 5.5, 2, 1
仮想アクセスポイントとネットワーク設定	Status	双方の無線インタフェースにおいて VAP0 が有効。他の VAP は無効。
	ネットワーク名 (SSID)	dlink1 から dlink16
	VLAN ID	1
	Broadcast SSID	許可
	セキュリティモード	None（プレーンテキスト）
	認証タイプ	None
	RADIUS IP アドレス	10.90.90.1
	RADIUS キー	secret
	RADIUS アカウンティング	無効
	HTTP Redirect	なし

設定項目		初期値
その他の設定	WDS	None
	STP	無効
	MAC 認証	リスト内にステーションの記載なし。
	Load Balancing	無効
	SNMP	有効
	RO SNMP Community Name	Public
	Managed AP Mode	無効
	認証（802.1X サプリカント）	無効
	Management ACL	無効
	HTTP Access	有効、「Managed Mode」では無効。
	HTTPS Access	有効、「Managed Mode」では無効。
	SNMP Agent Port	161
	SNMP Set Requests	無効
	Console Port Access	有効
	Telnet Access	有効、「Managed Mode」では無効。
	SSH Access	有効、「Managed Mode」では無効。
	WMM	有効
	Network Time Protocol (NTP)	有効
	Clustering	停止
	Client QoS Global Admin Mode	無効
	VAP QoS Mode	無効